Wireless Controller, Service Platform and Access Point

WiNG 7.2.0 CLI Reference Guide

9036356-00 Rev AA

Published July 2019

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

Open Source Declarations

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

Table of Contents

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.
New!	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]**
Words in italicized type	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 www.extremenetworks.com/documentation/). 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

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. 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, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks 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.
Call GTAC	For immediate support: 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

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

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).
3 Select the products for which you would like to receive notifications.

Note
You can modify your product selections or unsubscribe at any time.

4 Click **Submit**.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

1 About this Guide

Notational Conventions

This manual describes the *CLI (Command Line Interface)* commands and configurations required to bring up and deploy Extreme Networks' access points, wireless controllers and service platforms within a WiNG 7.2.0 managed network.

The WiNG 7.2.0 software supports the following access points and service platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Note
The 802.11ax AP5XX model access points are a part of the ExtremeWireless OmniEdge line of products.

WiNG 7.2.0 introduces the following <XXXX> ExtremeMobility access points:

-
-

The other ExtremeMobility AP5XX model access points supported by the WiNG 7.X.X software are:

- AP560h - This is a dual-radio, cloud-ready, stadium optimized, *Wi-Fi* 6, 802.11ax outdoor access point with eight internal antennas, supporting two internal antenna modes: *30 degree and 70 degree*. It is ideally suited for high-density user environments, such as stadiums, large public venues, convention centers and school auditoriums. The AP560h offers flexible deployment options and can be mounted under a seat, to a pole, and a wall, thereby ensuring exceptional mobile user experience.
- AP560i - This is a cloud-ready, stadium optimized, Wi-Fi 6, 802.11ax outdoor access point with two internal antenna. It is ideally suited for high-density user environments, such as stadiums, large public venues, convention centers and school auditoriums. The AP560i offers flexible deployment options and can be mounted under a seat, to a pole, and a wall, thereby ensuring exceptional mobile user experience.
- AP510e - This is a next generation, enterprise-class 802.11ax access point. The AP features a dual-band radio, a band locked radio, and comes with eight (8) Wi-Fi *external* antennas and one *Bluetooth Low Energy* (BLE) antenna.
- AP510i - This is a next generation, enterprise-class 802.11ax access point. The “i” in AP510i indicates that it comes with internal antennas. The AP features a dual-band radio, a band locked radio, and comes with eight (8) Wi-Fi internal antennas and one BLE antenna.
- AP505i - This is a next generation, enterprise-class 802.11ax access point. The “i” in AP505i indicates that it comes with internal antennas. The AP505i can be used in stadiums, public venues such as hospitals and hotels, retail industry, and educational institutions. The 802.11ax technology supports more users and *internet of things* (IoT) devices.

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

<variable>	Variables are described with a short description enclosed within a '<' and a '>' pair.
	For example, the command,
	`nx9500-6C8809>show interface ge 1`
	is documented as:
	`show interface ge <1-2>`
	where:
	• 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
	
	Note: Since this output is from an NX 9500 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.

|	The pipe symbol. This is used to separate the variables/keywords in a list.
	For example, the command,
	`nx9500-6C8809> show .....`
	is documented as:
	`show [adoption|bluetooth|bonjour|boot|.....`
	where:
	• show – is the command – displays information
	• [adoption|bluetooth|bonjour|boot|.....] – indicates the different keywords that can be combined with the *show* command. However, only one of the above option can be used at a time.
	
	`show adoption ...`
	`show bluetooth ...`
	`show bonjour ...`

[]	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,
	`nx9500-6C8809# clear ...`
	is documented as:
	`clear [arp-cache|bonjour|cdp|counters|crypto| event-history|firewall|gre|ip|ipv6|l2tpv3-stats|lacp| license|lldp|logging|mac-addresstable|mint|role|rtls| spanning-tree|traffic-shape|vrrp]`
	where:
	• clear – is the command
	• [arp-cache|bonjour|cdp|counters|crypto| .....|vrrp] – indicates that these keywords are available for this command. However, only one can be used at a time.

{ }	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.
	For example, the command,
	`nx9500-6C8809> show adoption ....`
	is documented as:
	`show adoption info *{on <DEVICE-NAME>}*`
	here:
	• show adoption info – is the command. This command can also be used as:
	`show adoption info`
	The command can also be extended as:
	`show adoption info *{on <DEVICE-NAME>}*`
	here:
	• {on <DEVICE-NAME>} – is the optional keyword.

command / keyword	The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.
	For example, the command,
	`nx9500-6C8809>show wireless`
	is documented as:
	`show wireless`
	where:
	• show – is the command
	• wireless – is the keyword

()	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.
	For example, the command,
	`crypto pki export request generate-rsa-key test autogen-subject-name ...`
	is documented as:
	`nx9500-6C8809#crypto pki export request generate-rsa-key test autogen-subject-name (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>)`
	here:
	• crypto pki export request generate-rsa-key <RSA-KEYPAIR-NAME> auto-gen-subject-name – is the command
	• <RSA-KEYPAIR-NAME> – is the RSA keypair name (in this example, the keypair name is 'test')
	• (<URL>,email <EMAIL>,fqdn <FQDN>,ip-address <IP>) – is the set of recursive parameters (separated by commas) that can be used in any order.

2 Introduction

WiNG 7.1.X Operating System Overview
CLI Overview

This chapter provides a general overview of the WiNG 7 operating system and the *CLI (Command Line Interface)* structure. It also provides a list of commands required to deploy and manage access points within the WiNG managed network.

WiNG 7.1.X Operating System Overview

The WiNG 7 operating system is a solution designed for 802.11n, 802.11ac and 802.11ax networking. It is a convergence of the legacy ExtremeWireless™ WiNG (5.9.X) and ExtremeWireless™ (10.X) wireless operating systems. It offers a high-level of flexibility and scalability covering both campus and distributed modes of deployment.

WiNG 7.1.X brings together the following key benefits of both deployment topologies under one fold:

- *ExtremeWireless* - The ExtremeWireless software provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points. It is an ideal solution for high-density, campus and stadium deployments. It is well suited to meet the needs of enterprises in the education, healthcare, sports and entertainment verticals. The ExtremeWireless OS key strengths are:
  - Extensive Policy Framework
  - Contextual Device and Application Control
  - Application Visibility & Control with Analytics
  - BYOD - Single *SSID* with Programmable Data Path
  - Voice & Video Optimized with Seamless Roaming
- *ExtremeWireless WiNG* - The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It is designed for standalone or distributed hierarchical networks. The ExtremeWireless WiNG software distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time. It is highly scalable and well suited to meet the needs of large, geographically distributed enterprises. It is an ideal wireless networking solution for the retail, manufacturing, transportation & logistics, and hospitality verticals. The ExtremeWireless OS key strengths are:
  - Simple Guest Access with Analytics
  - Contextual Application Control
  - Advanced Diagnostics and Remote Troubleshooting
  - Intrusion, Compliance and Wi-Fi Forensics
  - Scale-out 1000s of APs with Rapid Rollout

- Self-tuning RF (Smart-RF)
- Distributed Service Intelligence

Going forward, this unified, common, wireless, infrastructure WiNG 7.1 OS will power both ExtremeWireless and ExtremeWireless WiNG product families. The WiNG 7.1.2 OS supports the following platforms:

- Access Points - AP510i, AP505i, AP510e, AP560i, AP560h
- Service Platforms - NX5500, NX7500, NX9500, NX9600 and VX9000

Interoperability with WiNG 5.9.X

Interoperability with access points running the WiNG 5.9.X OS is another salient feature of the WiNG 7.1.X OS. As part of this inter-interoperability, WiNG 7.1.X wireless controllers and service platforms are capable of deploying and managing the following WiNG 5.9.X APs:

- Access Points - AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533

Dual Mode Capability

The WiNG 7 AP5XX (AP505, AP510 and AP560) model access points have the capability of operating in the **`Distributed`** and **`Centralized`** modes. For a newly-manufactured, out-of-the-box AP5XX model access point the mode of operation is not specified.

Note
For more information, see Dual Mode Capability.

AP560h Specifications

The enterprise class 802.11ax AP560h access point has the following features:

- Radios: 2 radios; 1 IoT radio (2.4 GHz).
- Console Port: RJ45.
- Two Ethernet Ports:
  - GE1 - 10/100/1000/2500/5000 Mbps auto-negotiation Ethernet port, RJ45, with *Power over Ethernet* PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
- LEDs: 2 – All LEDs will be on during reset
- One Reset button
- Power: PoE 802.3af; 12VDC external power in connector.
- Antennas:
  - Eight WiFi internal antennas, supporting the following internal antenna modes:
    30 degree
    70 degree
  - One BLE internal antenna

AP560i Specifications

The enterprise class 802.11ax AP560i access point has the following features:

- Radios: 2 radios; 1 IoT radio (2.4 GHz).
- Console Port: RJ45.
- Two Ethernet Ports:
  - GE1 - 10/100/1000/2500/5000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
- LEDs: 2 – All LEDs will be on during reset
- One Reset button
- Power: PoE 802.3af; 12VDC external power in connector.
- Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

AP510e Specifications

The enterprise class 802.11ax AP510e access point has the following features:

- Radios: 2 radios; 1 IoT radio (2.4 GHz).
- Console Port: RJ45.
- Two Ethernet Ports:
  - GE1 - 10/100/1000/2500/5000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
- LEDs: 6 – All LEDs will be on during reset
- One Reset button
- Power: PoE 802.3af; 12VDC external power in connector.
- Antennas:
  - Eight WiFi external antennas
  - One BLE internal antenna

AP510i Specifications

The enterprise class 802.11ax AP510i access point has the following features:

- Radios: 2 radios; 1 IoT radio (2.4 GHz).
- Console Port: RJ45.
- Two Ethernet Ports:
  - GE1 - 10/100/1000/2500/5000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
- LEDs: 6 – All LEDs will be on during reset
- One Reset button
- Power: PoE 802.3af; 12VDC external power in connector.
- Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

AP505i Specifications

The enterprise class 802.11ax AP505i access point has the following features:

- Radios: 2 radios (one band locked at 2.4 GHz and the other band at 5 GHz); 1 IoT radio (2.4 GHz)
- Console port: RJ45
- Two Ethernet ports:
  - GE1 - 10/100/1000/2500 Mbps auto-negotiation Ethernet port, RJ45, with PoE In
  - GE2 - 10/100/1000 Mbps auto-negotiation Ethernet port, RJ45, with NO PoE
- LEDs: 6 LEDs; all LEDs will be on during reset
- One reset button
- Power: PoE 802.3af; 12VDC external power in connector
- Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

Note
For more information on the AP505i, AP510i/e and AP560i/h, refer to the respective installation guides, available at https://extremenetworks.com/documentation.

CLI Overview

This section describes the commands available within a device's CLI structure. CLI is available for access points, wireless controller, and service platforms.

You can 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:

Bits Per Second	**19200** - For NX5500, NX7500, NX9500, NX9600, VX9000 model service platforms. **115200** - For AP505 and AP510 model access points
Data Bits	**8**
Parity	**None**
Stop Bit	**1**
Flow Control	**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 – NX 5500

The above example indicates the command is only available for a NX 5500 model wireless controller.

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.

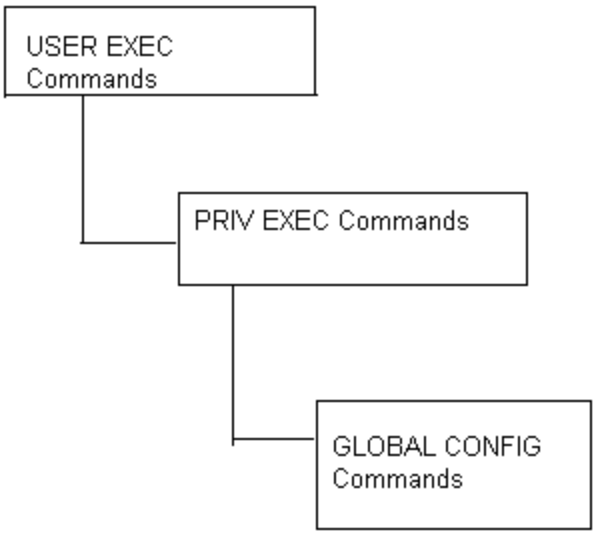


Figure 1: Figure: Hierarchy of User Modes

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.

```
ap505-13403B>
```

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.

```
ap505-13403B>en
ap505-13403B#
```

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.

```
ap505-13403B#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap505-13403B(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.

```
ap505-13403B(config)#aaa-policy test
ap505-13403B(config-aaa-policy-test)#
```

To enter the logged device's configuration, execute the following command:

```
ap505-13403B(config)#self
ap505-13403B(config-device-94-9B-2C-13-40-38)#
```

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	AP505
cluster	change-passwd	AP510
commit	clear	application
connect	clock	application-group
create-cluster	cluster	application-policy
crypto	commit	association-acl-policy
crypto-cmp-cert-update	configure	auto-provisioning-policy
database	connect	bgp
database-backup	copy	ble-data-export-policy
database-restore	cpe (supported on NX7500, NX9500, NX9600, and VX9000)	bonjour-gw-discovery-policy
debug	create-cluster	bonjour-gw-forwarding-policy
device-upgrade	crypto	bonjour-gw-query-forwarding-policy
disable	crypto-cmp-cert-update	captive-portal
enable	database	clear
file-sync	database-backup	client-identity
help	database-restore	client-identity-group
join-cluster	debug	clone

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
l2tpv3	delete	crypto-cmp-policy
logging	device-upgrade	customize
mint	diff	database-client-policy (supported only on VX9000)
no	dir	database-policy (supported only on NX9500, NX9600, and VX9000)
on	disable	device
opendns	edit	device-categorization
page		dhcp-server-policy
ping	enable	dhcpv6-server-policy
ping6	erase	dns-whitelist
revert	ex3500 (supported only on NX9500, NX9600, and VX9000)	event-system-policy
service	factory-reset	ex3500
show	file-sync	ex3500-management-policy
ssh	halt	ex3500-qos-class-map-policy
telnet	help	ex3500-qos-policy-map
terminal	join-cluster	ex3524
time-it	l2tpv3	ex3548
traceroute	logging	firewall-policy
traceroute6	mint	global-association-list
virtual-machine (supported only on NX9500, NX9600, and VX9000)	mkdir	guest-management
watch	more	help
write	no	host
clrscr	on	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 1167.
exit	opendns	inline-password-encryption
	page	iot-device-type-imagotag-policy
	ping	ip
	ping6	ipv6
	pwd	ipv6-router-advertisement-policy
	raid (supported only on NX9500, NX9600, and NX7500)	l2tpv3

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
	re-elect	location-policy
	reload	mac
	remote-debug	management-policy
	rename	meshpoint
	revert	meshpoint-qos-policy
	rmdir	mint-policy
	self	nac-list
	service	no
	set-personality	nsight-policy
	show	NX5500 (supported only on NX9500, NX9600, and VX900 and)
	ssh	NX7500 (supported only on NX9500, NX9600, and VX9000)
	t5 (supported only on RFS400, NX9500, NX9600, and VX9000)	NX9000 (supported only on NX9500, NX9600, and VX9000)
	telnet	NX9600 (supported only on NX9600, and VX9000)
	terminal	passpoint-policy
	time-it	password-encryption
	traceroute	profile
	traceroute6	radio-qos-policy
	upgrade	radius-group
	upgrade-abort	radius-server-policy
	virtual-machine (supported only on NX9500, NX9600 and VX9000)	radius-user-pool-policy
	watch	rename
		replace
	write	rf-domain
	clrscr	rfs4000
	exit	roaming-assist-policy
		role-policy
		route-map
		routing-policy
		rtl-server-policy
		schedule-policy
		self

Table 3: Controller CLI Modes and Commands (continued)

User Exec Mode	Priv Exec Mode	Global Configuration Mode
		sensor-policy
		smart-rf-policy
		t5 (supported only on NX7500, NX9500, NX9600 and VX9000
		url-filter (supported only on NX9500, NX9600, and VX9000)
		url-list (supported only on NX9500, NX9600 and VX9000)
		vx9000 (supported only on NX9500, NX9600, and VX9000)
		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

Command	Description
(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.

```
nx9500-6C8809#service?
  service  Service Commands

nx9500-6C8809#
```

```
ap505-13403B#se?
  self             Config context of the device currently logged into
  service          Service Commands
  set-personality  Change personality on next reload

ap505-13403B#
```

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.

```
nx9500-6C8809#service ?
  block-adopter-config-update       Block configuration updates from the
                                    adopter
  bluetooth                         Bluetooth service commands
  clear                             Reset functions
  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
  database                          Database Commands
  delete                            Delete sessions
  delete-offline-aps                Delete Access Points that are configured
                                    but offline
  eguest                            Guest commands
```

```
  force-send-config                 Resend configuration to the device
  force-update-vm-stats             Force VM statistics to be pushed up to the
                                    NOC
  guest-registration                Guest registration
  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
  nsight                            Nsight
  pktcap                            Start packet capture
  pm                                Process Monitor
  radio                             Radio parameters
  radius                            Radius test
  request-full-config-from-adopter  Request full configuration from the
                                    adopter
  restore                           Restore from a backup
  set                               Set global options
  show                              Show running system information
  signal                            Send a signal to a process
  smart-rf                          Smart-RF Management Commands
  snmp                              Snmp
  snmpv3                            Snmpv3
  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 service commands

nx9500-6C8809#
```

It is possible to abbreviate commands and keywords to allow a unique abbreviation. For example, "configure terminal" can be abbreviated as **config 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:

```
ap505-13403B>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?').

ap505-13403B>
```

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.

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

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:

```
nx9500-6C8809#conf[TAB]

nx9500-6C8809#configure

nx9500-6C8809#configure[ENTER]
Enter configuration commands, one per line.  End with CNTL/Z.
nx9500-6C8809(config)#
```

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:

```
nx9500-6C8809#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

nx9500-6C8809#
```

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 service platforms:
  - NX5500, NX7500, NX9500, NX9600, and VX9000
- a default profile for each of the following access points:
  - AP505 and AP510

You can modify a default profile. In the following example, an IP address is assigned to the management port on the default AP505 profile.

```
nx9500-6C8809(config)#profile ap505 default-ap505
nx9500-6C8809(config-profile-default-ap505)#interface me1
nx9500-6C8809(config-profile-default-ap505-if-me1)#ip address 172.16.10.2/24
nx9500-6C8809(config-profile-default-ap505-if-me1)#commit
nx9500-6C8809(config-profile-default-ap505)#exit
nx9500-6C8809(config)#
```

The following command displays a default ap505 profile configuration:

```
nx9500-6C8809(config-profile-default-ap505)#
nx9500-6C8809(config-profile-default-ap505)#show context
profile ap505 default-ap505
 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 radio1
 interface radio2
 interface bluetooth1
  shutdown
  mode le-sensor
 interface ge1
 interface ge2
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
--More--

nx9500-6C8809(config-profile-default-ap505)   #
```

Changing Default Profile

This section describes how to change the default profile by creating vlan 150 and mapping to ge1 physical interface.

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

```
nx9500-6C8809(config-profile-default-ap505)#interface vlan 150
nx9500-6C8809(config-profile-default-ap505-if-vlan150)#ip address 192.168.150.20/24
nx9500-6C8809(config-profile-default-ap505-if-vlan150)#exit
nx9500-6C8809(config-profile-default-ap505)#interface ge 1
nx9500-6C8809(config-profile-default-ap505-if-ge1)#switchport access vlan 150
```

```
nx9500-6C8809(config-profile-default-ap505-if-ge1)#commit write memory
[OK]
nx9500-6C8809(config-profile-default-ap505-if-ge1)#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

nx9500-6C8809(config-profile-default-ap505-if-ge1)#
```

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.

```
ap505-13403B>en
ap505-13403B#
```

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

```
ap505-13403B#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap505-13403B(config)#
```

3 Go to ‘default-management-policy’ mode.

```
ap505-13403B(config)#management-policy ?
  MANAGEMENT  Name of the management policy to be configured (will be created
              if it does not exist)

ap505-13403B(config)#management-policy default
ap505-13403B(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.

```
ap505-13403B(config-management-policy-default)#telnet
ap505-13403B(config-management-policy-default)#commit write
ap505-13403B(config-management-policy-default)#end
ap505-13403B#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.

```
ap505-13403B(config-management-policy-default)#user testuser password test@123
 role helpdesk access all
ap505-13403B(config-management-policy-default)#commit
ap505-13403B(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
ap505-13403B(config-management-policy-default)#
```

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.

```
ap505-13403B>en
ap505-13403B#
```

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

```
ap505-13403B#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap505-13403B(config)#
```

3 Go to ‘default-management-policy’ mode.

```
ap505-13403B(config)#management-policy ?
  MANAGEMENT  Name of the management policy to be configured (will be created
              if it does not exist)
```

```
ap505-13403B(config)#management-policy default
ap505-13403B(config-management-policy-default)#
```

4 Enter SSH at the command prompt.

```
ap505-13403B(config-management-policy-default)#ssh
ap505-13403B(config-management-policy-default)#commit write
ap505-13403B(config-management-policy-default)#end
ap505-13403B#exit
```

5 Connect to the access point 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.

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

```
ap505-13403B(config-management-policy-default)#user testuser password test@123
 role helpdesk access all
ap505-13403B(config-management-policy-default)#commit
ap505-13403B(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
ap505-13403B(config-management-policy-default)#
```

3 User Exec Mode Commands

user-exec-commands

Logging in to the wireless controller or access point 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 on page 33	Uploads captive portal advanced pages
change-password on page 36	Changes the password of a logged user
clear on page 37	Resets the last saved command
clock on page 51	Configures the system clock
cluster on page 52	Accesses the cluster context
commit on page 53	Commits changes made in the active session.
connect on page 53	Establishes a console connection to a remote device
create-cluster on page 64	Creates a new cluster on a specified device
crypto on page 54	Enables encryption
crypto-cmp-cert-update on page 65	Triggers a CMP certificate update on a specified device or devices
database on page 66	Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)
database-backup on page 70	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server
database-restore on page 71	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 on page 72	Configures device firmware upgrade settings
enable on page 78	Turns on (enables) the privileged mode command set
join-cluster on page 84	Adds a device (access point, wireless controller, or service platform) to an existing cluster of devices
file-sync on page 78	Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points
help on page 81	Describes the interactive help system.
l2tpv3 on page 85	Establishes or brings down L2TPv3 *(Layer 2 Tunneling Protocol Version 3)* tunnels
logging on page 87	Modifies message logging facilities

Table 4: User Exec Mode Commands (continued)

Command	Description
mint on page 88	Configures MiNT protocol
no on page 90	Negates a command or sets its default
on on page 91	Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show
opendns on page 91	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 on page 95	Toggles a device's (Access Point, wireless controller, or service platform) paging function
ping on page 96	Sends ICMP echo messages to a user-specified location
ping6 on page 97	Sends ICMPv6 echo messages to a user-specified location
ssh on page 98	Opens an SSH connection between two network devices
telnet on page 99	Opens a Telnet session
terminal on page 100	Sets the length and width of the terminal window
time-it on page 101	Verifies the time taken by a particular command between request and response
traceroute on page 101	Traces the route to its defined IPv4 destination
traceroute6 on page 102	the route to its defined IPv6 destination
watch on page 109	Repeats a specific CLI command at a periodic interval
virtual-machine on page 103	Installs, configures, and monitors the status of VMs *(virtual machines)*. This command is specific to the NX 9500 and NX 9510 series service platforms.
exit on page 110	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 616.

Note

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

captive-portal-page-upload

Uploads *captive portal* 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.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <CAPTIVE-PORTAL-NAME> – Specify captive portal's name (should be existing and configured).
<MAC/HOSTNAME>	Uploads to a specified AP • <MAC/HOSTNAME> – Specify the AP's MAC address or hostname.
all	Uploads to all APs
upload-time <TIME>	Schedules an AP upload time • <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 web pages of the captive portal identified by the <CAPTIVE-PORTAL-NAME> parameter • <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 • <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 web pages to APs via the controller to which the APs are adopted
upload-time <TIME>	Optional. Schedules an AP upload time • <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 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:
	• <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
	  • <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 pages
<CAPTIVE-PORTAL-NAME> <FILE-NAME>	Identifies the captive-portal and Web pages to delete • <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 web pages
<CAPTIVE-PORTAL-NAME> <URL>	Specify the captive portal's name and location. The captive portal should be existing and configured. IPv4 URLs: • 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: • 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 **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.

Examples

```
ap510-133B3B#captive-portal-page-upload load-file captive_portal_test tftp://89.89.89.17/
pages_new_only.tar
ap510-133B3B#show captive-portal-page-upload load-file-status
Download of captive_portal_test advanced page file is complete
ap510-133B3B#
ap510-133B3B#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
-------------------------------------------------------------------------------------
  ap510-133B3B   downloading   immediate   100      0       -                 None
-------------------------------------------------------------------------------------
ap510-133B3B#
```

change-password

Changes the password of the logged user.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
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

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
clear [arp-cache|bonjour|cdp|counters|crypto|event-history|firewall|gre|ip|ipv6|l2tpv3-stats|lacp|license|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 [all|ap|bridge|interface|radio|router|thread|wireless-client]
clear counters all {(on <DEVICE-OR-DOMAIN-NAME>)}
clear counters [bridge|router|thread]
clear counters interface <INF-TYPE> {(on <DEVICE-OR-DOMAIN-NAME>)}
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 firewall [dhcp|dos|flows|neighbors]
clear firewall [dhcp|neighbors] snoop-table {on <DEVICE-NAME>}
clear firewall [dos stats|flows [ipv4|ipv6]] {on <DEVICE-NAME>}
clear gre stats {on <DEVICE-NAME>}
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 license [borrowed|lent to <BORROWER-CONTROLLER-NAME>] {on <DEVICE-NAME>}
clear l2tpv3-stats tunnel <TUNNEL-NAME> {session <SESSION-NAME>} {on <DEVICE-NAME>}
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 • <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 • <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)* 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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear counters all {(on <DEVICE-OR-DOMAIN-NAME>)}
```

counters	Clears all counters on the logged device or on all devices within a specified RF Domain. These counters are: AP, bridge, interface, radio, router, thread and wireless clients.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Specify the device name or the RF Domain name. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears all counters on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. Note: If you do not specify a device name or an RF Domain name, the system clears all counters on the logged device.

```
clear counters [bridge|router|thread]
```

counters	Clears counters based on the parameters passed. The options are: AP, bridge, interface, radio, router, thread and wireless clients.
[bridge|router|thread]	Select one of the following options: • bridge – Clears bridge counters. When executed, this command resets the bridge forwarding cache. • router – Clears router counters. When executed, this command resets the router counters. • thread – Clears thread counters. When executed, this command resets the pre-thread counters.

```
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, bridge, interface, radio, router, thread and wireless clients.
ap <MAC>	Clears counters for all APs or a specified AP • <MAC> – Optional. Specify the AP's MAC address. Note: If no MAC address is specified, all AP counters are cleared.
radio <MAC/DEVICE-NAME> <1-X>	Clears radio interface counters on a specified device or on all devices • <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. Note: If no device name or MAC address is specified, all radio interface counters are cleared.

wireless-client <MAC>	Clears counters for all wireless clients or a specified wireless client • <MAC> – Optional. Specify the wireless client's MAC address. Note: If no MAC address is specified, all wireless client counters are cleared.
on <DEVICE-OR-DOMAIN-NAME>	The following option is common to all of the above keywords: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Clears AP, radio, or wireless client counters on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
clear counters interface <INF-TYPE> <INF-NUMBER>{(on <DEVICE-OR-DOMAIN-NAME>)}
```

counters	Clears counters based on the parameters passed. The options are: AP, bridge, interface, radio, router, thread and wireless clients.
interface <INF-TYPE> <INF-NUMBER>	Clears interface counters • <INF-TYPE> - Specify the interface type as Ethernet, VLAN, port-channel, usb, all, etc. • <INF-NUMBER> - After specifying the interface type, specify the interface number.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Clears the specified interface counters on a specified device 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 *Internet Key Exchange* (IKE) *security associations* (SAs) • <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 • <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/IPsec-ESP/IPsec-AH* database SAs • 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 gre stats {on <DEVICE-NAME>}
```

gre stats	Clears GRE tunnel statistics
on <DEVICE-NAME>	Optional. Clears GRE tunnel statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
clear event-history
```

event-history	Clears event history cache entries

```
clear firewall [dhcp|neighbors] snoop-table {on <DEVICE-NAME>}
```

firewall	Clears configured wireless firewall filter statistics based on the parameters passed
[dhcp|neighbors] snoop-table	Clears the following snoop-table database • dhcp - Clears the *DHCP (Dynamic Host Configuration Protocol)* snooping binding database. • neighbors - Clears *IPv6* neighbor cache.
on <DEVICE-NAME>	The following option is common to both the 'dhcp' and 'neighbor' parameters: • on <DEVICE-NAME> - Optional. Executes the command on as specified device. • <DEVICE-NAME> - Specify the AP, wireless controller, or service platform name.

```
clear firewall [dos stats|flows [ipv4|ipv6]] {on <DEVICE-NAME>}
```

firewall	Clears configured wireless firewall filter statistics based on the parameters passed
dos stats	Clears *DoS* statistics

flows [ipv4|ipv6]	Clears all established IPv4 or IPv6 firewall session statistics • ipv4 - Optional. Clears only IPv4 firewall session statistics • ipv6 - Optional. Clears only ipv6 firewall session statistics Note: If you do not specify IPv4 or IPv6, the system clears all ACL related statistics.
on <DEVICE-NAME>	The following option is common to both the 'dos' and 'flows' parameters: • on <DEVICE-NAME> - Optional. Executes the command on as specified device. • <DEVICE-NAME> - Specify the AP, wireless controller, or service platform name.

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

ip bgp [<IP>|all|external]	Clears on-going *BGP (Border Gateway Protocol)* sessions based on the option selected • <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 This command is applicable only to the NX9500, NX9600, and VX9000 platforms. 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.
in prefix-filter	Optional. Clears inbound route updates • prefix-filter – Optional. Clears the existing *Outbound Route Filtering* (ORF) prefix-list
on <DEVICE-NAME>	Optional. Clears route updates on a specified device • <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]	Clears on-going *BGP* sessions based on the option selected • <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 This command is applicable only to the NX9500, NX9600, and VX9000 platforms.
out	Optional. Clears outbound route updates. Optionally specify the device on which to execute this command.
on <DEVICE-NAME>	The following keyword is recursive and optional. • on <DEVICE-NAME> – Optional. Clears BGP sessions on a specified device • <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]	Clears on-going *BGP* sessions based on the option selected • <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 This command is applicable only to the NX9500, NX9600, and VX9000 platforms.
soft {in|out}	Optional. Initiates soft-reconfiguration of route updates for the specified IP address • in – Optional. Enables soft reconfiguration of inbound route updates • out – Optional. Enables soft reconfiguration of outbound route updates 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.
on <DEVICE-NAME>	Optional. Initiates soft reconfiguration inbound/outbound route updates on a specified device • <DEVICE-NAME> – Specify the name of the AP or service platform.

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

ip bgp process	Clears all BGP processes running This command is applicable only to the NX9500, NX9600, and VX9000 platforms.
on <DEVICE-NAME>	Optional. Clears all BGP processes on a specified device • <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>	Optional. Clears a specified address binding or all address bindings on a specified device • <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 OSPF *(Open Shortest Path First)* 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. • <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 • <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/statistics for a specified channel group or all channel groups configured • <1-4> counters – Clears LACP stats for a specified channel group. Specify the port-channel index number from 1 - 4. Note, LACP is supported only on the NX5500, NX7500, NX9500, and NX9600 model service platforms. However, the NX9500 series service platforms support only two (2) channel groups, and the other model service platforms support four (4) channel groups. • counters – Clears LACP stats for all configured channel groups on the device

```
clear license [borrowed|lent to <BORROWER-CONTROLLER-NAME>] {on <DEVICE-NAME>}
```

license	Releases borrowed licenses or revokes lent licenses
borrowed	Releases all licenses borrowed by the logged controller or by a specified controller **Note:** If you do not specify a controller name, the command is executed on the controller you have logged on to.
lent to <BORROWING-CONTROLLER-NAME>	Revokes licenses lent to a specified controller • to <BORROWING-CONTROLLER-NAME> - Specifies the borrowing controller's name. When specified, the system revokes all licenses (AP, AAP) lent to the specified controller.

on <DEVICE-NAME>	Optional. This option is common to both of the above parameters.
	• on <DEVICE-NAME> - Specify the name of the controller on which the command is to be executed.
	  • <DEVICE-NAME> – Specify the name of the wireless controller or service platform.
	  Note:
	  If you do not specify the controller name, the system executes the command on the logged controller.

```
clear l2tpv3-stats tunnel <TUNNEL-NAME> {session <SESSION-NAME>} {on <DEVICE-NAME>}
```

l2tpv3-stats	Clears L2TPv3 tunnel statistics for a specified L2TPv3 tunnel
tunnel <TUNNEL-NAME>	Specifies the tunnel name

session <SESSION-NAME>	Optional. Clears a specific session statistics in the specified L2TPv3 tunnel. • <SESSION-NAME> - Specify the session name. Note: If you do not specify the session name, the system clears statistics for all sessions.
on <DEVICE-NAME>	This option is common to all of the above parameters. • on <DEVICE-NAME> - Optional. Executes the command on a specified device. • <DEVICE-NAME> - Specify the name of the AP, wireless controller, or service platform. Note: If you do not specify the device name, the system clears L2TPv3 tunnel and session statistics on the logged 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. • <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 Note: If executed without specifying any MAC address(es), all MAC addresses from the MAC address table will be removed.
vlan <1-4094>	Optional. Clears all MAC addresses for a specified VLAN • <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 • <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) • <IF-NAME> – Specify the layer 2 interface name.
ge <1-X>	Clears MAC address forwarding table for the specified GigabitEthernet interface • <1-X> – Specify the GigabitEthernet interface index from 1 - X. Note: The number of GE interfaces supported varies for different device types.
port-channel <1-X>	Clears MAC address forwarding table for the specified port-channel interface • <1-X> – Specify the port-channel interface index from 1 - X. Note: The number of port-channel interfaces supported varies for different device types.
on <DEVICE-NAME>	Optional. Clears the MAC address forwarding table, for the selected interface, on a specified device • <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>	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. • <MAC> – Specify the MAC address to clear. • 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>	Optional. Clears the specified MAC address on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: If a device is not specified, the system clears the MAC address on all devices.

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

mint	Clears MiNT related information
mlcp history	Clears *MiNT Link Creation Protocol* (MLCP) client history
on <DEVICE-NAME>	Optional. Clears MLCP client history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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

role ldap-stats	Clears *Lightweight Directory Access Protocol* (LDAP) server statistics
on <DEVICE-NAME>	Optional. Clears LDAP server statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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

rtls	Clears *Real Time Location Service* (RTLS) statistics
aeroscout	Clears RTLS Aeroscout statistics
ekahau	Clears RTLS Ekahau statistics
<MAC/DEVICE-NAME>	This keyword is common to the 'aeroscout' and 'ekahau' parameters. • <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>	This keyword is common to the 'aeroscout' and 'ekahau' parameters. • 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>	Optional. Clears spanning tree entries on a specified device • <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]	Optional. Clears spanning tree entries on different interfaces • <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 *Switch Virtual Interface* (SVI) VLAN ID from 1- 4094. • wwan1 – Clears detected spanning tree entries for wireless WAN interface.
on <DEVICE-NAME>	Optional. Clears spanning tree entries on a specified device • <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 • <1-4> – Specify the traffic class from 1 - 4. **Note:** If the traffic class is not specified, the system clears all traffic shaping statistics.
on <DEVICE-NAME>	Optional. Clears traffic shaping statistics for the specified traffic class on a specified device • <DEVICE-NAME> – Specify the name of the access point, wireless controller, or service platform.

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

vrrp	Clears *VRRP (Virtual Router Redundancy Protocol)* statistics
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: • 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

```
ap510-133B3B>show event-history
EVENT HISTORY REPORT
Generated on '2019-01-08 13:31:16 UTC' by 'admin'

2019-01-08 13:07:43     ap510-133B3B  SYSTEM     LOGIN                Successfully logged
in user 'admin' with privilege 'superuser' from 'conso'
2019-01-01 00:02:00     ap510-133B3B  SYSTEM     COLD_START           System Cold start.
System came up at Jan 01 00:02:00 2019
2019-01-01 00:00:27     ap510-133B3B  NSM        IFUP                 Interface ge1 is up
2019-01-01 00:00:26     ap510-133B3B  NSM        IFUP                 Interface ge1 is up
2019-01-01 00:00:23     ap510-133B3B  DIAG       NEW_LED_STATE        LED state message
RADIO_2_52G_LED_ON from module DOT11
2019-01-01 00:00:23     ap510-133B3B  RADIO      RADIO_STATE_CHANGE   Radio
'ap510-133B3B:R2' changing state from 'Initializing' to 'On'
2019-01-01 00:00:23     ap510-133B3B  DIAG       NEW_LED_STATE        LED state message
RADIO_2_52G_LED_ON from module DOT11
2019-01-01 00:00:23     ap510-133B3B  RADIO      RADIO_STATE_CHANGE   Radio
'ap510-133B3B:R2' changing state from 'On' to 'Initializing'
2019-01-01 00:00:23     ap510-133B3B  DIAG       NEW_LED_STATE        LED state message
RADIO_1_24G_NOT_CONFIG from module DOT11
2019-01-01 00:00:23     ap510-133B3B  RADIO      RADIO_STATE_CHANGE   Radio
'ap510-133B3B:R1' changing state from 'Initializing' to 'Off(no wlans mapped)'
--More--
ap510-133B3B>

ap510-133B3B>clear event-history

ap510-133B3B>show event-history
EVENT HISTORY REPORT
Generated on '2019-01-08 13:32:20 UTC' by 'admin'
ap510-133B3B>
```

clock

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. We recommend that you reset the local time zone on the device prior to setting the clock.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
ap510-133B3B(config-device-94-9B-2C-13-3B-3B)#America/Los_Angeles
ap510-133B3B>clock set 00:46:06 8 Jan 2019
ap510-133B3B>show clock
2019-01-08 00:51:34 PST
ap510-133B3B>
```

cluster

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:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cluster start-election
```

Parameters

```
cluster start-election
```

start-election	Starts a new cluster master election

Examples

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

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap510-133B3B#commit
[OK]
ap510-133B3B#
```

connect

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <MINT-ID> – Specify the remote device's MiNT ID.
<REMOTE-DEVICE-NAME>	Connects to the remote system using its name • <REMOTE-DEVICE-NAME> – Specify the remote device's name.

Examples

```
ap510-133B3B>connect
ap510-133B3B ap510-13452A default/ap510-133B3B default/ap510-13452A mint-id
ap510-133B3B>
ap510-133B3B>connect ap510-13452A
Entering character mode
Escape character is '^]'.
AP510 release 7.0.0.0-0009X
ap510-13452A login:
```

crypto

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 CSR *(Certificate Signing Request)*.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|zeroise]
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 • <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 • <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: • 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
	• <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.
	
	  After specifying the key size, optionally specify the device (access point or controller) to generate the key on.

on <DEVICE-NAME>	Optional. Generates the new RSA Keypair on a specified device • <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 • <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 • <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: • 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 • <RSA-KEYPAIR-NAME> – Specify the RSA Keypair name. Note: All device certificates associated with this key will also be deleted.
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: • 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 PKI *(Private Key Infrastructure)* management. Use this command to authenticate, export, generate, or delete a trustpoint and its associated CA *(Certificate Authority)* certificates.
authenticate <TRUSTPOINT-NAME>	Authenticates a trustpoint and imports the corresponding CA certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name.
url	Specify CA's location. Both IPv4 and IPv6 address formats are supported. Note: The CA certificate is imported from the specified location.

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: • 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 • 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 • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified FQDN *(Fully Qualified Domain Name)* • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system • <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
	• 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
	  • 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
	  • <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 • <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 • <SEND-TO-EMAIL> – Specify the CA's e-mail address.
fqdn <FQDN>	Exports CSR to a specified FQDN • <FQDN> – Specify the CA's FQDN.
ip-address <IP>	Exports CSR to a specified device or system • <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, CRL *(Certificate Revocation List)*, server certificate, and private key • <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 • <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: • 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 • <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 • 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 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 • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN • <FQDN> – Specify the FQDN.

ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system • <IP> – Specify the device's IP address.
on <DEVICE-NAME>	Optional. Exports the self-signed certificate 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> 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 • <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 • 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.
subject-name <COMMON-NAME>	Configures a subject name, defined by the <COMMON-NAME> keyword, to identify the certificate • <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 • <SEND-TO-EMAIL> – Specify the e-mail address.
fqdn <FQDN>	Optional. Exports the self-signed certificate to a specified FQDN • <FQDN> – Specify the FQDN.
ip-address <IP>	Optional. Exports the self-signed certificate to a specified device or system • <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, CRL, or a trustpoint to the selected device
[certificate|crl] <TRUSTPOINT-NAME>	Imports a signed server certificate or CRL • 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: • 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 • <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 • <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: • 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, 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 • <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: • 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

```
ap510-133B3B#crypto key generate rsa local 2048 on ap510-133B3B
RSA Keypair successfully generated
ap510-133B3B#
```

create-cluster

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:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <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 • <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 • 1 – Configures level 1 (local) routing • 2 – Configures level 2 (inter-site) routing

Examples

```
nx9500-6C8809#create-cluster name TechPubs1 ip 192.168.13.8 level 2
... creating cluster
... committing the changes
... saving the changes
Please Wait .
[OK]
nx9500-6C8809#
nx9500-6C8809#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
nx9500-6C8809#
```

Related Commands

cluster on page 52	Initiates cluster context. The cluster context provides centralized management to configure all cluster members from any one member.
join-cluster on page 84	Adds an access point, wireless controller or service platform, as a member, to an existing cluster of controllers

crypto-cmp-cert-update

Triggers a CMP *(Certificate Management Protocol)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.

Examples

```
NOC-NX9500#crypto-cmp-cert-update test on B4-C7-99-71-17-28
CMP Cert update success
NOC-NX9500#
```

database

Enables automatic repairing (vacuuming) and dropping databases. Also enables keyfile generation.

If enforcing authenticated access to a 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 — NX9500, NX9600, VX9000

Syntax

```
database [drop|keyfile|repair]
database drop [all|captive-portal]
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]
```

database drop [all|captive-portal|]	Drops (deletes) all or a specified database. Execute the command on the device hosting the database. • all – Drops all databases, captive portal and NSight • captive-portal – Drops the captive-portal 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 623. 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.

Examples

```
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 and set up the onboard database. Note, the example uses replica set database deployment.

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 WiNG device hosting the captive-portal database)

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 S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
```

```
Primary-DB-HOST(config-database-policy-techpubs)#show context
database-policy techpubs
 authentication
 authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/
Ih2ruxnOYnr
 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 Use the database policy created in the previous step on the primary database.

```
Primary-DB-HOST(config-device-B4-C7-99-6C-88-09)#use database-policy techpubs
```

5 In the database-client policy context

Note
This configuration is needed in deployments implementing captive-portal registration and database authentication with an onboard database.

a Configure the user credentials created in Step 1 d.

```
NOC-Controller(config-database-client-policy-techpubs)#authentication username
techpubs password S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/Ih2ruxnOYnr
```

b View the configuration.

```
NOC-Controller(config-database-client-policy-techpubs)#show context
database-client-policy techpubs
 authentication username techpubs password 2 S540QFZz9LzSOdX1ZJEqDgAAAAy3b7GtyO4Z/
Ih2ruxnOYnr
NOC-Controller(config-database-client-policy-techpubs)#
```

6 Use the database client policy configured in the previous step on the WiNG device that will access the database.

```
<DB-CLIENT>(config-device-B4-C7-99-6C-88-09)#use database-client-policy techpubs
```

Related Commands

database-backup on page 70	Backs up all databases to a specified location and file on an FTP or SFTP server
database-restore on page 71	Restores a previously exported databases
database-policy global config on page 299	Documents database-policy configuration commands. Use this option to enable a WiNG device as the database.
database-client-policy global-config on page 296	Documents database-client-policy configuration commands. The database-client-policy is only needed in deployments implementing captive-portal registration and database authentication with an onboard database. Use this command to enable the controller or RF Domain manager to authenticate with the database.
service on page 623	Documents the database user account configuration details

database-backup

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 — NX9500, NX9600, VX9000

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: • 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 • <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

Examples

```
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>
```

Related Commands

database on page 66	Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and/or NSight)
database-restore on page 71	Restores a previously exported (backed up) database (captive-portal and/or NSight)]

database-restore

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 — NX9500, NX9600, VX9000

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: • 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

Examples

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

Related Commands

database on page 66	Enables automatic repairing (vacuuming) and dropping of databases (captive-portal and NSight)
database-backup on page 70	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server

device-upgrade

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
device-upgrade [<MAC/HOSTNAME>|all|ap505|ap510|ap560|nx5500|nx7500|nx9500|nx9600|vx9000|
cancel-upgrade|load-image|rf-domain]

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

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

device-upgrade [ap505|ap510|ap560|nx5500|nx7500|nx9500|nx9600|vx9000]
[all|containing <SUB-STRING>] {force|no-reboot|reboot-time <TIME>|
upgrade-time <TIME> {no-reboot|reboot-time <TIME>}}

device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap505|ap510|ap560|nx5500|nx7500|nx9500|
nx9600|vx9000|on rf-domain [<RF-DOMAIN-NAME>|all]]

device-upgrade load-image [ap505|ap510|ap560|nx5500|nx7500|nx9500|nx9600|vx9000]
 {<IMAGE-URL>|on <DEVICE-OR-DOMAIN-NAME>}

device-upgrade rf-domain [<RF-DOMAIN-NAME>|all|containing <WORD>|
filter location <WORD>] [all|ap505|ap510|ap560|nx5500|nx7500|nx9500|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 • <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 • <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 and specifies the time at which the device is to be upgraded
	• <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:
	  • 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 • <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
	• <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:
	  • 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. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade [ap505|ap510|ap560|nx5500|nx7500|nx9500|nx9600|vx9000]
[all|containing <SUB-STRING] {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: AP510, AP505, AP560, NX5500, NX7500, NX9500, NX9600, VX9000 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 • <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
	• <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:
	  • 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. • Optional. Enables staggered reboot (one at a time), without network impact

```
device-upgrade cancel-upgrade [<MAC/HOSTNAME>|all|ap505|ap510|ap560|nx5500|nx7500|nx9500|
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: • 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 • <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: ap510 and ap505
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 • <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 [ap505|ap510|ap560|nx5500|nx7500|nx9500|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. • <DEVICE-TYPE> - Specify the device type. The options are: AP510, AP505, AP560, AP560, NX5500, NX7500, NX9500, NX9600, VX9000. After specifying the device type, provide the location of the required device firmware image.
<IMAGE-URL>	Specify the device's firmware image location in one of the following formats: IPv4 URLs: • 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: • 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. • <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|ap505|ap510|ap560|nx5500|nx7500|nx9500|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>]	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. • <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>	After specifying the RF Domain, select the device type. The options are: AP510, AP505, AP560, NX5500, NX7500, NX9500, NX9600, VX9000. 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.

<MAC/HOSTNAME>	Optional. Use this option to identify specific devices (by their MAC address/ Hostnames) that are to be upgraded. 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. Note: If no MAC address or hostname is specified, all devices of the type selected are upgraded.
force	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.
from-controller	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.
no-reboot {staggered-reboot}	Optional. Disables automatic reboot after a successful upgrade (the device must be manually restarted)
reboot-time <TIME> {staggered-reboot}	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 common to all of the above. Optional. Enables staggered reboot (one at a time) without network impact

upgrade-time <TIME> {no-reboot| reboot-time <TIME>}	Optional. Schedules an automatic firmware upgrade
	• <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.
	  • 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.

Examples

```
nx9500-6C8809#show adoption status
-------------------------------------------------------------------------------------------
-----
DEVICE-NAME    VERSION       CFG-STAT      MSGS   ADOPTED-BY    LAST-ADOPTION    UPTIME
-------------------------------------------------------------------------------------------
------
ap8432-070235 5.9.4.0-015D  configured       No  nx9500-6C8809  0 days 00:22:49 9 days
22:53:56
ap7562-84A224 5.9.4.0-010D  configured       No  nx9500-6C8809  0 days 00:22:47 45 days
14:26:08
ap7532-DF9A4C 5.9.4.0-010D  configured       No  nx9500-6C8809  0 days 00:22:47 22 days
14:17:30
ap505-134038  7.1.0.0-128D  version-mismatch No  nx9500-6C8809  0 days 00:22:47 1 days
00:40:37
-------------------------------------------------------------------------------------------
-------
```

```
Total number of devices displayed: 4
nx9500-6C8809#
nx9500-6C8809>device-upgrade ap505-134038
--------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
--------------------------------------------------------------------------------
  B4-C7-99-6C-88-09         Success         Queued 1 devices to upgrade
--------------------------------------------------------------------------------
nx9500-6C8809>
nx9500-6C8809#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 ERROR
UPGRADED BY
------------------------------------------------------------------------------------------------
-----------
 ap505-134038 downloading immediate  immediate   11       0       -
nx9500-6C8809
------------------------------------------------------------------------------------------------
-----------
nx9500-6C8809#
```

enable

Turns on (enables) the privileged mode command set. The prompt changes from `ap510-133B3B>` to `ap510-133B3B#`. This command does not do anything in the Privilege Executable mode.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
enable
```

Parameters

```
None
```

Examples

```
ap510-133B3B>enable
ap510-133B3B#
```

file-sync

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

When enabling file syncing, consider the following points:

- The X.509 certificate needs synchronization only if the adopted devices are configured to use EAP-TLS authentication.
- Execute the command on the controller adopting the devices.
- 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>]`.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

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

file-sync cancel [trustpoint <TRUSTPOINT-NAME>| wireless-bridge] [<DEVICE-NAME>| all|rf-domain [<DOMAIN-NAME>| all]]	Cancels scheduled file synchronization • trustpoint – Cancels scheduled trustpoint synchronization on a specified device, all devices, or devices within a specified RF Domain • <TRUSTPOINT-NAME> - Specify the trustpoint name. • wireless-bridge – Cancels scheduled wireless-bridge certificate synchronization on a specified device, all devices, or devices within a specified RF Domain • <DEVICE-NAME> – Cancels scheduled trustpoint/certificate synchronization on a specified device. Specify the device's hostname or MAC address. • all – Cancels scheduled trustpoint/certificate synchronization on all devices • rf-domain [<DOMAIN-NAME>|all] – Cancels scheduled trustpoint/certificate synchronization on all devices in a specified RF Domain or in all RF Domains <DOMAIN-NAME> – Cancels scheduled trustpoint/certificate synchronization 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>}
```

file-sync trustpoint <TRUSTPOINT-NAME> [<DEVICE-NAME>| all|rf-domain [<DOMAIN-NAME> |all] from-controller]	Configures file-syncing parameters
	• trustpoint <TRUSTPOINT-NAME> – Syncs a specified trustpoint between controller and its adopted devices
	  • <TRUSTPOINT-NAME> – Specify the trustpoint name.
	
	Note: Trustpoint are synced all the way down the hierarchical structure. If you issue the command on the NOC controller, the specified trustpoint will be synced all the way down the site controllers and their adopted APs.
	• wireless-bridge – Syncs wireless-bridge certificate between controller and its adopted devices
	
	After specifying the file that is to be synced, configure following file-sync parameters:
	  • <DEVICE-NAME> – Syncs trustpoint/certificate with a specified AP. Specify the device's hostname or MAC address.
	  • all – Syncs trustpoint/certificate with all devices
	  • rf-domain [<DOMAIN-NAME>|all] from-controller – Syncs trustpoint/certificate with all devices in a specified RF Domain or in all RF Domains
	<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
	from-controller – Optional. Loads certificate to the APs from the adopting controller and not the RF Domain manager
	
	After specifying the access points, specify the following options: **reset-radio** and **upload-time**.

reset-radio	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'.
upload-time <TIME>	This keyword is recursive and applicable to all of the above parameters. • upload-time – Optional. Schedules certificate upload at a specified time • <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.

Examples

```
<CONTROLLER>#file-sync wireless-bridge ap510-133B3B upload-time 06/01/2019-12:30
-------------------------------------------------------------------------------
          CONTROLLER               STATUS                  MESSAGE
-------------------------------------------------------------------------------
     B4-C7-99-6D-B5-D4           Success           Queued 1 APs to upload
-------------------------------------------------------------------------------
<CONTROLLER>#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <WORD> – 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.
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>
nx9500-6C8809help 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>
```

join-cluster

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:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • 1 – Configures level 1 routing • 2 – Configures level 2 routing
mode [active|standby]	Optional. Configures the cluster mode • 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)

```
nx9500-6C8809>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]
nx9500-6C8809>

nx9500-6C8809>show context
!
! Configuration of RFS4000 version 7.1.0.0-075D
!
!
version 2.6
!
!
.....................................................................................
 cluster name TechPubs
 cluster mode standby
 cluster member ip 192.168.13.15 level 1
 logging on
 logging console warnings
 logging buffered warnings
!
!
end
nx9500-6C8809>
```

Related Commands

create-cluster on page 64	Creates a new cluster on the specified device
cluster on page 52	Initiates cluster context. The cluster context enables centralized management and configuration of all cluster members from any one member.

l2tpv3

Establishes or brings down a L2TPv3 *(Layer 2 Tunnel Protocol Version 3)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • 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 • <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 • <TUNNEL-NAME> – Specify the tunnel name. • session <SESSION-NAME> – Identifies a specific session <SESSION-NAME> – Specify the session name. down – Brings down the session identified by the <SESSION-NAME> keyword up – Establishes the session identified by the <SESSION-NAME> keyword
on <DEVICE-NAME>	Optional. Establishes or brings down a tunnel session on a specified device • <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 • down – Brings down all tunnels • up – Establishes all tunnels
on <DEVICE-NAME>	Optional. Establishes or brings down all tunnels on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx9500-6C8809>l2tpv3 tunnel testTunnel session testSession1 up on ap505-13403
```

Note
For more information on the L2TPV3 tunnel configuration mode and commands, see L2TPv3 Policy on page 1700.

logging

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.

Examples

```
ap505-13403B(config-device-94-9B-2C-13-40-38)#logging on
ap505-13403B>logging monitor debugging
ap505-13403B>show logging

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

Log Buffer (1932 bytes):


Jan 01 12:10:49 2019: %KERN-4-WARNING: [43292.697857] PRNG seed file updated.
Jan 01 03:30:28 2019: %KERN-4-WARNING: [12072.182963] jffs2: warning: (1353)
jffs2_sum_write_data: Summary too big (-32 data, -3733 pad) in eraseblock at 01d80000.
Jan 01 00:36:28 2019: %DATAPLANE-4-DOSATTACK: IPSPOOF ATTACK:  Source IP is Spoofed : Src
IP : 134.141.244.23, Dst IP: 10.234.160.36, Src Mac: 00-04-96-9C-F1-25, Dst Mac:
94-9B-2C-13-40-38, Proto = 6.
Jan 01 00:36:28 2019: %KERN-4-WARNING: [ 1632.268856]
Jan 01 00:19:35 2019: %KERN-4-WARNING: [  618.484856]
Jan 01 00:15:13 2019: %KERN-4-WARNING: [  356.442855]
Jan 01 00:13:10 2019: %KERN-4-WARNING: [  234.342855]
--More--
ap505-13403B>
```

Related Commands

no on page 90 no on page 160	Resets terminal lines logging levels

mint

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <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 • <1-60> – Specify a value from 1 - 10000. The default is 3.
size <1-64000>	Optional. Sets the MiNT payload size in bytes • <1-64000> – Specify a value from 1 - 640000. The default is 64 bytes.
timeout <1-10>	Optional. Sets a response time in seconds • <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 • <MINT-ID> – Specify the destination device's MiNT ID.
destination-port <1-65535>	Optional. Sets the *Equal-cost Multi-path* (ECMP) routing destination port • <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 • <1-255> – Specify a value from 1 - 255. The default is 30.
source-port <1-65535>	Optional. Sets the ECMP source port • <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 • <1-65535> – Specify a value from 1 sec - 255 sec. The default is 30 seconds.

Examples

```
nx9500-6C8809#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
nx9500-6C8809#
```

no

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.

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

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

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <RF-DOMAIN-NAME> – Specify the RF Domain name. Enters the specified RF Domain context. • all – Specifies all RF Domains.

Examples

```
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)>
```

opendns

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 Enabling OpenDNS Support.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

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. • <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 554.

```
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. • <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 • <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. • <LABEL> – Specify your network label. 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 554.

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 = 001480fe36dcb245#
```

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

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
page
```

Parameters

None

Examples

```
nx9500-6C8809#page
nx9500-6C8809#
```

Related Commands

no on page 90	Disables paging
no on page 160	Disables paging

ping

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

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

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 • <1-10000> – Specify a value from 1 - 10000. The default is 5.
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. • count <1-10000> – Optional. Sets the pings to the specified destination from 1 - 10000. The default is 5. • size <1-64000> – Optional. Sets the ping payload size from 1 - 64000 bytes. The default is 100 bytes.

size <1-64000>	Optional. Sets the ping payload size in bytes • <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes.
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. • <IP> – Specifies the source IP address • pppoe – Selects the PPP over Ethernet interface • vlan <1-4094> – Selects the VLAN interface from 1 - 4094 • wwan – Selects the wireless WAN interface

Examples

```
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>
```

ping6

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-10000> – Specify a value from 1 - 10000. The default is 5.
size <1-64000>	Optional. Sets the IPv6 ping payload size in bytes • <1-64000> – Specify the ping payload size from 1 - 64000. The default is 100 bytes.

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 1175 (profile config mode).

Examples

```
nx9500-6C8809(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
--------------------------------------------------------------------------------
nx9500-6C8809(config-device-00-23-68-1B-35-96-if-ge4)#

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

ssh

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-13403B#ssh 10.234.160.5 admin
admin@10.234.160.5's password:
nx9500-6C8809>
```

telnet

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <IP/HOSTNAME> – Specify the remote system's IPv4 or IPv6 address or hostname.
<TCP-PORT>	Optional. Specify the *Transmission Control Protocol* (TCP) port number.
<INTF-NAME>	Optional. Specify the interface name for the link local address.

Examples

```
nx9500-6C8809#telnet 10.234.160.36

Entering character mode
Escape character is '^]'.


AP505 release 7.1.0.0-114D
ap505-13403B login:
```

terminal

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <0-512> – Specify a value from 0 - 512.
width <0-512>	Sets the width (the number of characters displayed) of the terminal window • <0-512> – Specify a value from 0 - 512.

Examples

```
ap505-13403B#show terminal
Terminal Type: xterm
Length: 0     Width: 80
ap505-13403B#
ap505-13403B#terminal length 30
ap505-13403B#terminal width 100
ap505-13403B#show terminal
Terminal Type: xterm
Length: 30     Width: 100
ap505-13403B#
```

Related Commands

no on page 90	Resets the width or length of the terminal window
no on page 160	Resets the width or length of the terminal window

time-it

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-13403B#time-it config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
That took 0.00 seconds..
ap505-13403B(config)#
```

traceroute

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.

Examples

```
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

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
traceroute6 <LINE>
```

Parameters

```
traceroute6 <LINE>
```

traceroute6 <LINE>	Traces the route to a destination IPv6 address or hostname • <LINE> – Specify the destination IPv6 address or hostname.

Examples

```
nx9500-6C88097#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
nx9500-6C8809#
```

virtual-machine

Installs, configures, and monitors the status of *virtual machines*

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 — NX9500, NX9600, VX9000

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>|team-urc|team-rls|team-vowlan]
virtual-machine restart [<VM-NAME>|hard|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 VX9000 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>|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. • 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 l2 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 NX9500 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.
	• 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>|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. • 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>|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. • 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>|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. • 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>
```

virtual-machine volume-group [add-drive|resize-drive] <BLOCK-DEVICE-LABEL>]	Enables provisioning of logical volume-groups on the VX9000 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 VX9000 installation and cannot be added to existing VX9000 installation. • add-drive – 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 `show > virtual-machine > volume-group > status` command. • resize-drive - 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 `show > virtual-machine > volume-group > status` command. The following keyword is common to all of the above parameters: • <BLOCK-DEVICE-LABEL> –Specify the block-device label to be added or resized depending on the action being performed.

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

virtual-machine volume-group replace-drive <BLOCK-DEVICE-LABEL> <NEW-BLOCK-DEVICE-LABEL>]	Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives. • replace-drive – 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 `show > virtual-machine > volume-group > status` command • <BLOCK-DEVICE-LABEL> –Specify the block-device label to be replaced. <BLOCK-DEVICE-LABEL> – Specify the replacement block-device label.

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

virtual-machine volume-group resize-volume-group <BLOCK-DEVICE-LABEL>	Enables provisioning of VMs as logical volume-groups on the VX9000 platform. Logical volume-group VMs are created on the primary storage device, allowing the database storage to be expanded to include additional storage drives • resize-volume-group – Adds drive space to an existing block-device in the volume-group • <BLOCK-DEVICE-LABEL> –Specify the block-device label to which additional drive space is to be provided

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-DE6F97>cirtual-machine add-drive sdb
VX-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-DE6F97>
```

watch

Repeats the specified CLI command at periodic intervals

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

exit

Ends the current CLI session and closes the session window

For more information, see exit.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
exit
```

Parameters

```
None
```

Examples

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

4 Privileged Exec Mode Commands

privileged-exec-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 1534.

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
  operational-mode              Change personality on next reload
  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
archive on page 115	Manages file archive operations
boot on page 117	Specifies the boot partition as primary or secondary. The device boots using the image stored in the specified partition.
captive-portal-page-upload on page 33	Uploads captive portal advanced pages to adopted access points
cd on page 118	Changes the current directory
change-password on page 36	Changes the password of the currently logged-in user
clear on page 37	Clears parameters, cache entries, table entries, and other similar entries
clock on page 51	Configures the system clock
cluster on page 52	Initiates a cluster context
configure on page 119	Enters the global configuration mode
commit on page 53	Commits changes made in the active session.
connect on page 53	Begins a console connection to a remote device
copy on page 120	Clears parameters, cache entries, table entries, and other similar entries
cpe on page 120	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.
create-cluster on page 64	Creates a new cluster on a specified device
crypto on page 54	Enables encryption
crypto-cmp-cert-update on page 65	Triggers a CMP certificate update on a specified device or devices
database on page 66	Enables automatic repairing (vacuuming) and dropping of databases (Captive-portal and NSight)
database-backup on page 70	Backs up captive-portal and/or NSight database to a specified location and file on an FTP or SFTP server
database-restore on page 71	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.
delete on page 122	Deletes a specified file from the system
device-upgrade on page 72	Configures device firmware upgrade parameters
diff on page 123	Displays the differences between two files
dir on page 124	Displays the list of files on a file system
disable on page 125	Disables the privileged mode command set
edit on page 125	Edits a text file
erase on page 126	Erases a file system
ex3500 on page 129	Enables the EX3500 switch firmware management. Use this command to perform the following operations: boot, copy, delete, and IP related configurations.

Table 5: Privileged Exec Commands (continued)

Command	Description
factory-reset on page 136	Erases startup configuration on a specified device or all devices within a specified RF Domain Note: Use this command to revert an AP505 and AP510 model access points personality flag to 'unknown'.
file-sync on page 78	Configures parameters enabling syncing of PKCS#12 and wireless-bridge certificate between the staging-controller and adopted access points
help on page 81	Describes the interactive help system.
halt on page 141	Halts a device (access point, wireless controller, or service platform)
join-cluster on page 84	Adds a device (access point, wireless controller, or service platform), as cluster member, to an existing cluster of devices
l2tpv3 on page 85	Establishes or brings down L2TPV3 tunnels
logging on page 87	Modifies message logging parameters
mint on page 88	Configures MiNT settings
mkdir on page 142	Creates a new directory in the file system
more on page 142	Displays the contents of a file
no on page 160	Negates a command or sets its default
on on page 91	Executes the following commands in the RF Domain context: clrscr, do, end, exit, help, service, and show
opendns on page 91	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.
operational-mode on page 143	Resets a standalone AP's mode of operation from 'distributed' to 'centralized'. Note: This command is only applicable on AP505, AP510 and AP560 model access points.
page on page 95	Toggles a device's (access point, wireless controller, or service platform) paging function
ping on page 96	Sends ICMP echo messages to a user-specified location
ping6 on page 97	Sends ICMPv6 echo messages to a user-specified location
pwd on page 144	Displays the current directory
re-elect on page 145	Re-elects the tunnel controller (wireless controller, service platform, or access point)
reload on page 145	Halts a device (wireless controller, service platform, or access point) and performs a warm reboot
rename on page 151	Renames a file in the existing file system
rmdir on page 152	Deletes an existing file from the file system
self on page 153	Displays the configuration context of the device

Table 5: Privileged Exec Commands (continued)

Command	Description
ssh on page 98	Connects to another device using a secure shell
t5 on page 153	Executes the following operations on a T5 device: copy, rename, delete, and write. This command is specific to the NX95XX and NX96XX devices.
telnet on page 99	Opens a Telnet session
terminal on page 100	Sets the length and width of the terminal window
telnet on page 99	Verifies the time taken by a particular command between request and response
time-it on page 101	Verifies the time taken by a particular command between request and response
traceroute on page 101	Traces the route to a defined IPv4 destination
traceroute6 on page 102	Traces the route to a defined IPv6 destination
upgrade on page 155	Upgrades the software image
upgrade-abort on page 158	Aborts an ongoing software image upgrade
exit on page 110	Ends the current CLI session and closes the session window
watch on page 109	Repeats the specific CLI command at a periodic interval
virtual-machine on page 103	Installs, configures, and monitors the status of VMs. This command is specific to the NX95XX and NX96XX series service platforms.
raid on page 159	Enables RAID management. This command is specific to the NX95XX and NX96XX series service platforms.

Note
For information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Common Commands on page 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

Changes the next boot partition or image on a specified device or on the logged device. The WiNG devices have two partitions: primary and secondary, with each partition containing an image of the operating system. Whenever the device boots up it loads the image from the partition specified here.

The partition currently in control of the boot process is the active partition, the other partition is the inactive partition with the alternate image. Use this command to manually change the next boot partition or image.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

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

Parameters

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

system [active|inactive|primary|secondary]	Specifies the image used by the device to boot up • active – Changes the next boot image to the current, running (active) image • inactive – Changes the next boot image to the current, inactive image • primary – Changes the next boot partition to the primary partition. • secondary – Changes the next boot partition to the secondary partition. Note: You will need to reload the device in order for the change to take effect.
on <DEVICE-NAME>	Optional. Changes the next boot image or partition on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: If no device is specified, the logged device's next boot-up configuration is changed.

Examples

```
ap505-13403B#show boot
------------------------------------------------------------------------------
    IMAGE           BUILD DATE            INSTALL DATE            VERSION
------------------------------------------------------------------------------
  Primary      02/14/2019 19:48:51    01/01/1970 00:00:00    7.0.0.0-0001X
  Secondary    02/13/2019 09:44:05    01/01/2019 00:08:50    7.1.0.0-105T
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Secondary
Software Fallback  : Enabled
ap505-13403B#
ap505-13403B#boot system primary
Updated system boot partition
ap505-13403B#
ap505-13403B#show boot
------------------------------------------------------------------------------
    IMAGE           BUILD DATE            INSTALL DATE            VERSION
------------------------------------------------------------------------------
  Primary      02/14/2019 19:48:51    01/01/1970 00:00:00    7.0.0.0-0001X
  Secondary    02/13/2019 09:44:05    01/01/2019 00:08:50    7.1.0.0-105T
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Primary
Software Fallback  : Enabled
ap505-13403B#
```

cd

Changes the current directory

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-13403B#cd flash:/log/
ap505-13403B#pwd
flash:/log/
ap505-13403B#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-13403B#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap505-13403B(config)#
nx9500-6C8809#configure self
Enter configuration commands, one per line.  End with CNTL/Z.
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

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 recommended that you 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.

```
ap505-13403B#c#copy flash:/log/upgrade.log tftp://10.233.89.183:/upgrade.log
Accessing running-config file from remote TFTP server into switch running-config.
ap505-13403B#c#copy tftp://10.233.89.183:/running-config running-config
```

cpe

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:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 #unique_122.

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 • <1-24> – Reloads only those CPEs whose IDs have been specified. Specify the ID from 1 - 24. • all – Reloads all CPEs
[primary|secondary]	Select the next boot image • primary – Uses the primary image when reloading • secondary – Uses the secondary image when reloading
on <T5-DEVICE-NAME>	Optional. Performs this operation on a specified T5 device • <T5-DEVICE-NAME> – Specify the T5 device's hostname.

```
cpe [reload|upgrade <IMAGE-LOCATION>] cpe [<1-24>|all] {on <T5-DEVICE-NAME>}
```

cpe [reload| upgrade <IMAGE-LOCATION>]	Performs the following operations on CPEs • reload – Reloads the device • upgrade <IMAGE-LOCATION> – Upgrades the device • <IMAGE-LOCATION> – Specify the location of the firmware image. Both IPv4 and IPv6 addresses are supported. Use one of the following options to provide the location: IPv4 URLs: • 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: • 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 **Note:** After specifying the operation to perform, identify the device(s).
cpe [<1-24>|all]	Identifies the CPE(s) on which the operation is performed • <1-24> – Configures the CPE's ID from 1 - 24 • all – Configures all CPEs
on <T5-DEVICE-NAME>	Optional. Performs this operation on a specified T5 device • <T5-DEVICE-NAME> – Specify the T5 device's hostname.

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#
```

delete

Deletes a specified file from the device's file system

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 • Deletes the file specified by the <FILE> parameter

Examples

```
nx9500-6C8809#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y
nx9500-6C8809

nx9500-6C8809#delete /force flash:/tmp.txt

nx9500-6C8809#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
nx9500-6C8809
```

diff

Displays the differences between two files on a device's file system or a particular URL

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-13403B#diff startup-config running-config
--- startup-config
```

```
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
 !
 ! Configuration of AP505 version 7.1.0.0-105T
 !
@@ -81,13 +82,10 @@
 rf-domain default
  no country-code
 !
-self
-! ap505 94-9B-2C-13-40-38
- radio-count 2
+ap505 94-9B-2C-13-40-38
  use profile default-ap505
  use rf-domain default
  hostname ap505-13403B
- no adoption-site
  ip default-gateway 10.234.160.254
  interface ge1
   switchport mode access
ap505-13403B#
```

dir

Lists files on a device's file system

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dir {/all|/recursive|<DIR>|all-filesystems}
```

Parameters

```
dir {/all|/recursive|<DIR>|all-filesystems}
```

/all	Optional. Lists all files
/recursive	Optional. Lists files recursively
<DIR>	Optional. Lists files in the named file path
all-filesystems	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-filesystems
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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
disable
```

Parameters

None

Examples

```
nx9500-6C8809#disable
nx9500-6C8809>
ap505-13403B#disable
ap505-13403B>
```

edit

Edits a text file on the device's file system

ap505-13403B#dis ap505-13403B>

Syntax

```
edit <FILE>
```

Parameters

```
edit <FILE>
```

<FILE>	Specify the name of the file to modify.

Examples

```
ap505-13403B#edit startup-config
  GNU nano 1.2.4               File: startup-config

!
! Configuration of AP505 version 7.1.0.0-114D
!
!
version 2.6
!
!
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 $
 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 114 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
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 **<HOSTNAME/MAC>** or **on <DOMAIN-NAME>** 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>}	Optional. Erases the startup configuration file on all devices or specified device(s) in a specified RF Domain • <DOMAIN-NAME> – 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: • containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname <SUB-STRING> – Specify the sub-string to match. The startup configuration file is erased on all devices whose hostname contains the sub-string specified here. • exclude-controllers – Optional. Executes the command on all devices excluding controllers. The startup configuration file is erased on all devices except controllers. • 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. • filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type. <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 7622, AP7632, AP7662, AP-8163, AP-8432, AP-8533, RFS 4000, NX 5500, NX 7500, NX 95XX, NX 96XX, and VX. 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.

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#
```

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 — NX9500, NX9600, VX9000

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. Note: To view an EX3500's current image version, use the `show > version > on <EX3500-DEVICE-NAME>` 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 • <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname.

```
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. Note: As of now only one (1) EX3500 unit can be managed through a NOC controller.
(config|opcode) <FILE-NAME>	The following keywords are recursive: Specifies the image file to use for booting. The options are: • config – Uses the configuration file to boot the switch • opcode – Uses the opcode *(Operation Code)*, 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. The following parameter is common to the 'config' and opcode' keywords: • <FILE-NAME> – Specify the configuration/runtime-code file name.
on <EX3500-DEVICE-NAME>	Reloads a specified EX3500 switch • <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. You can also specify its MAC address.

```
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>	Copies a specified file (this is the source configuration file) • file – Copies the specified source file to a specified file (this is the destination configuration file) • <SOURCE-FILE-NAME> – Specify the source configuration file's name <DEST-FILE-NAME> – Specify the destination configuration file's name. When specifying the destination file name, keep in mind the following points: - It should not contain slashes (\ or /), - It should not exceed 32 characters for files on the switch, or 127 characters for files on the server.
on <EX3500-DEVICE-NAME>	Copies the file to a specified EX3500 switch • <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.

```
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]	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. This command also allows you to add a remote system's running configuration to the current system configuration.
add-to-running-config	Adds a remote system's running configuration to the current system
<FTP/TFTP-SERVER-IP> <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. • <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format. • <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user) <PASSWORD> – Specify the password applicable for the above specified FTP server user name.
<SOURCE-FILE-NAME>	After specifying the server details, specify the name of the running configuration file. • <SOURCE-FILE-NAME> – Specify the source file's name.
on <EX3500-DEVICE-NAME>	Copies the file to a specified EX3500 switch • <EX3500-DEVICE-NAME> – Specify the EX3500 switch's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.

```
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> <USER-NAME> <PASS-WORD>	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. • <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format. • <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user) <PASSWORD> – Specify the password applicable for the above specified FTP server user name.
[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. • [1|2] – Select the file type from 1 - 2. • 1 – Copies the EX3500 configuration file. • 2 – Copies the opcode, which is the runtime code. The opcode is like an operating system that enables the EX3500 software to communicate with the EX3500 device. <SOURCE-FILE-NAME> – Specify the source file's name. <DEST-FILE-NAME> – Specify the destination file's name.
on <EX3500-DEVICE-NAME>	Copies the file to a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname. The specified source file is copied to specified destination file on the EX3500 identified here.

```
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> <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. • <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format. • <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user) <PASSWORD> – Specify the password applicable for the above specified FTP server user name.

<SOURCE-CERT-FILE-NAME> <SOURCE-PVT-KEY-FILE-NAME> <PVT-PASS-WORD>	After identifying the FTP or TFTP server, specify the following: • <SOURCE-CERT-FILE-NAME> – Specify the source HTTPS secure site certificate file name. • <SOURCE-PVT-KEY-FILE-NAME> – Specify the source private-key file name. <PVT-PASS-WORD> – Specify the private password.
on <EX3500-DEVICE-NAME>	Copies the file to a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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> <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. • <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format. • <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user) <PASSWORD> – Specify the password applicable for the above specified FTP server user name.
[1|2] <SOURCE-PUB-KEY-FILE-NAME> <USER-NAME>	After identifying the FTP or TFTP server, specify the following: • [1|2] – Configures the SSH public key type as RS or DSA • 1 – Configures the public key type as RSA • 2 – Configures the public key type as DSA <SOURCE-PUB-KEY-FILE-NAME> – Specifies the source public key file name <USER-NAME> – Specifies the public key's user name
on <EX3500-DEVICE-NAME>	Copies the public key to a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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 The running configuration file can be copied to the startup configuration file and vice versa.

<FTP/TFTP-SERVER-IP> <USER-NAME> <PASSWORD>	If copying to a FTP/TFTP server, configure the following parameters: • <FTP/TFTP-SERVER-IP> – Specify the FTP or TFTP server's IP address in the A.B.C.D format. • <USER-NAME> – If using a FTP server, specify the FTP server's user name (should be an authorized user) <PASSWORD> – Specify the password applicable for the above specified FTP server user name.
<DEST-FILE-NAME>	Configures the destination file name. The running or startup configuration file is copied to the specified destination file. • <DEST-FILE-NAME> – Specify the destination file name. You can also copy the running configuration file to the startup configuration file and vice versa.
on <EX3500-DEVICE-NAME>	Copies the running or startup configuration file on to a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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]	Copies the file system from the EX3500 switch identified by the unit number • <1-1> – Specify the unit number from 1 - 1. • [1|2] – Select the file type from 1 - 2. 1 – Copies the selected unit's configuration file. • 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.
<SOURCE-FILE-NAME>	Configures the source file name • <SOURCE-FILE-NAME> – Specify the source file name. You can copy the running configuration file to the startup configuration file and vice versa.
<DEST-FILE-NAME>	Configures the destination file name. The running or startup configuration file is copied to the specified file. • <DEST-FILE-NAME> – Specify the destination file name. You can copy the running configuration file to the startup configuration file and vice versa.
on <EX3500-DEVICE-NAME>	Copies the running or startup configuration file on to a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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. • <FILE-NAME> – Specify the file name.

unit <1-1> name <FILE-NAME>	Identifies the unit in the stackable system on which the file is located • <1-1> – Select the unit from 1 - 1. • name – After identifying the unit, specify the file to delete. The specified file is deleted. <FILE-NAME> – Specify the file name.
on <EX3500-DEVICE-NAME>	Executes the command on a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
ex3500 delete public-key <USER-NAME> [dsa|rsa] on <EX3500-DEVICE-NAME>
```

ex3500 delete public-key <USER-NAME> [dsa|rsa]	Deletes a specified user's public key • <USER-NAME> – Specify the SSH user's name. • dsa – Deletes the specified user's DSA (version 2) key • rsa – Deletes the specified user's RSA (version 1) key
on <EX3500-DEVICE-NAME>	Executes the command on a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
ex3500 ip ssh crypto host-key generates [dsa|rsa] on <EX3500-DEVICE-NAME>
```

ex3500 ip ssh crypto host-key generates [dsa|rsa]	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. • dsa – Generates DSA (version 2) key type • rsa – Generates RSA (version 1) key type Note: The RSA Version 1 is used only for SSHv1.5 clients, whereas DSA Version 2 is used only for SSHv2 clients. Note: 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 `ex3500 > ip > ssh > save > host-key` command.
on <EX3500-DEVICE-NAME>	Executes the command on a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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>	Executes the command on a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

```
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>	Executes the command on a specified EX3500 device • <EX3500-DEVICE-NAME> – Specify the EX3500 device's hostname.

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 based on the parameters passed.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
factory-reset [config-all|config-device-only|deep|on <RF-DOMAIN-NAME>]
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>}]
factory-reset deep <AP-HOSTNAME>
factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|
exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

Parameters

```
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>}]
```

[config-all| config-device-only]	Erases startup configuration and reloads only controller-adopted devices. • config-all – Erases startup configuration on all adopted devices or on specified adopted devices. Issue the command on the controller or virtual controller AP. To execute the command on a specified device, provide the device hostname/MAC address. Note: This option also removes the device's configuration staged on the adopting controller. • config-device-only – Erases only the startup configuration on all adopted devices or on specified adopted devices. Issue the command on the controller or virtual controller AP. To execute the command on a specified device, provide the device hostname/MAC address. Note: This option only erases the startup configuration. It does not remove the device's configuration staged on the adopting controller. Note: For more information on the actions performed by this command, click here.
<HOSTNAME/MAC> {<HOSTNAME/MAC>}	This parameter is common to the 'config-all' and 'config-device-only' keywords: • <HOSTNAME/MAC> – Erases startup configuration and reloads the device identified by the <HOSTNAME/MAC> keyword. Specify the device's hostname or MAC address. • <HOSTNAME/MAC> – Optional. You can optionally specify multiple space-separated devices.
on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>	The following parameters are common to the 'config-all' and 'config-device-only' keywords: • on <RF-DOMAIN-NAME> – Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain • <RF-DOMAIN-NAME> – 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: containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname <SUB-STRING> – Specify the sub-string to match. 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. 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. filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type

	<DEVICE-TYPE> – Specify the device type. The options are: AP510, AP505.

```
factory-reset deep <AP-HOSTNAME>
```

deep	Resets an adopted AP's mode of operation to factory-default setting (that is not specified). Issue the command on the adopting WiNG VC/Controller and specify the AP' hostname. Once the AP's mode of operation is reverted to factory-default setting, the AP reboots and moves into the discovery mode to determine its mode of operation. The WiNG 7.1 AP505 and AP510 model access points have the capability of operating in the following two modes: **Distributed** and **Centralized**. For a newly-manufactured, out-of-the-box AP505 and AP510 access point the mode of operation is not specified. Note: For more information on operational modes and how it is set, see Dual Mode Capability.
<AP-HOSTNAME>	Specify the hostname of the AP on which the deep reset is to be implemented.

```
factory-reset on <RF-DOMAIN-NAME> {containing <SUB-STRING>|exclude-controllers|
exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

factory-reset	Erases startup configuration and reloads device(s) based on the parameters passed Note: For more information on the actions performed by this command, click here.
on <RF-DOMAIN-NAME> {containing <SUB-STRING>| exclude-controllers| exclude-rf-domain-manager| filter <DEVICE-TYPE>]}	Erases startup configuration and reloads all devices or specified device(s) within a specified RF Domain identified by the <RF-DOMAIN-NAME> keyword • <RF-DOMAIN-NAME> – 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: • containing <SUB-STRING> – Optional. Executes the command on all devices containing a specified sub-string in their hostname <SUB-STRING> – Specify the sub-string to match. • 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. • 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. • filter <DEVICE-TYPE> – Optional. Executes the command on all devices of a specified type <DEVICE-TYPE> – Specify the device type. The options are: AP510, AP505, RFS4000, NX5500, NX7500, NX9500, NX9600, and VX9000. The startup configuration is erased on all devices of the type specified here. For example, if AP510 is the device-type specified, the command is executed on all AP510s within the specified RF Domain.

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

```
nx9500-6C8809#factory-reset config-device-only ap505-134038
In progress ....
Erased startup-config - success 1 fail 0
Successful device deletion - total 1
nx9500-6C8809#
nx9500-6C8809#factory-reset deep ap505-13403B
In progress ....
reset ap deep - success 1 fail 0
Successful device deletion - total 1
nx9500-6C8809#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Specifies the name of the device to be halted • <DEVICE-NAME> – Enter the name of the AP, wireless controller, or service platform. **Note:** If the device name is not specified, the logged device is halted.

Example

```
nx9500-6C8809#halt on rfs4000-229D58
nx9500-6C8809#
```

mkdir

Creates a new directory in the file system

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
nx9500-6C8809#dir
Directory of flash:/.

  drwx             Thu Sep 27 07:10:45 2018   tmptpd
  drwx             Thu Sep 27 07:10:45 2018   floorplans
  drwx             Wed Feb 27 11:24:42 2019   crashinfo
  drwx             Thu Sep 27 07:11:07 2018   hotspot
  drwx             Thu Sep 27 07:10:45 2018   cache
  drwx             Mon Feb 25 20:13:56 2019   archived_logs
  drwx             Wed Feb 27 02:53:06 2019   log
  drwx             Thu Sep 27 07:10:45 2018   upgrade

nx9500-6C8809#
nx9500-6C8809#mkdir test
nx9500-6C8809#dir
Directory of flash:/.

  drwx             Thu Sep 27 07:10:45 2018   tmptpd
  drwx             Thu Sep 27 07:10:45 2018   floorplans
  drwx             Wed Feb 27 11:24:42 2019   crashinfo
  drwx             Wed Feb 27 13:42:52 2019   test
  drwx             Thu Sep 27 07:11:07 2018   hotspot
  drwx             Thu Sep 27 07:10:45 2018   cache
  drwx             Mon Feb 25 20:13:56 2019   archived_logs
  drwx             Wed Feb 27 02:53:06 2019   log
  drwx             Thu Sep 27 07:10:45 2018   upgrade

nx9500-6C8809#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
more <FILE>
```

Parameters

```
more <FILE>
```

<FILE>	Specify the file name and location. Provide the complete path to the file.

Examples

```
ap505-13403B#more flash:/archived_logs/startup.2.log
00-09-44-01-01-19
Jan 01 00:09:44 2019: %KERN-6-INFO: [    0.000000] Booting Linux on physical CPU 0x0.
Jan 01 00:09:44 2019: %KERN-5-NOTICE: [    0.000000] Linux version 4.1.51-ws-symbol (wios-
eng@wios-build) (gcc version 5.3.0 (GCC) ) #1 SMP Wed Feb 13 04:42:41 EST 2019.
Jan 01 00:09:44 2019: %KERN-4-WARNING: [    0.000000] CPU: AArch64 Processor [420f1000]
revision 0.
Jan 01 00:09:44 2019: %KERN-6-INFO: [    0.000000] Detected VIPT I-cache on CPU0.
Jan 01 00:09:44 2019: %KERN-6-INFO: [    0.000000] alternatives: enabling workaround for
ARM erratum 845719.
Jan 01 00:09:44 2019: %KERN-5-NOTICE: [    0.000000] Memory limited to 1022MB.
Jan 01 00:09:44 2019: %KERN-4-WARNING: [    0.000000] We are in the primary kernel.
Jan 01 00:09:44 2019: %KERN-6-INFO: [    0.000000] crashkernel successfully reserved:
0x0000000008000000 - 0x000000000b000000 (48 MB).
Jan 01 00:09:44 2019: KERN: [    0.000000] On node 0 totalpages: 259584.
Jan 01 00:09:44 2019: KERN: [    0.000000]   DMA zone: 4088 pages used for memmap.
Jan 01 00:09:44 2019: KERN: [    0.000000]   DMA zone: 0 pages reserved.
Jan 01 00:09:44 2019: KERN: [    0.000000]   DMA zone: 259584 pages, LIFO batch:31.
--More--
ap505-13403B#
```

operational-mode

Resets a WiNG standalone AP's mode of operation from 'distributed' or 'centralized'.

The WiNG 7.1 AP505 and AP510 model access points have the capability of operating in the following two modes: **`Distributed`** and **`Centralized`**. For a newly-manufactured, out-of-the-box AP505 and AP510 access point the mode of operation is not specified.

Note
For more information on the dual modes of operation, see Dual Mode Capability.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Syntax

```
operational-mode centralized
```

Parameters

```
operational-mode centralized
```

operational-mode centralized	Resets the WiNG standalone AP's mode of operation to: • centralized - In the *Centralized* mode ExtremeWireless AP models AP505i and AP510i adopt to the ExtremeCloud Appliance. A Centralized site topology allows seamless roaming within one geographic location. For more information, please refer to the ExtremeCloud Appliance User Guide available at https://extremenetworks.com/documentation. **Note:** After issuing the command, reload the AP for the change to take effect.

Examples

```
ap505-134038#operational-mode centralized
ap505-134038#reload
The system will be rebooted, do you want to continue? (y/n): y
ap505-134038#
```

pwd

Displays the full path of the present working directory, similar to the UNIX pwd command

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
pwd
```

Parameters

```
None
```

Examples

```
ap505-13403B#pwd
flash:/
ap505-13403B#
ap505-13403B#dir
Directory of flash:/.

  drwx             Thu Jan  1 00:00:07 1970   floorplans
  drwx             Thu Jan  1 00:00:07 1970   cache
  drwx             Tue Jan  1 00:09:01 2019   wipslog
  drwx             Tue Feb 26 14:43:27 2019   log
  drwx             Tue Feb 26 14:39:01 2019   archived_logs
  drwx             Thu Jan  1 00:00:07 1970   upgrade
```

```
  drwx             Thu Jan  1 00:00:07 1970   tmptpd
  drwx             Wed Feb 20 18:23:39 2019   crashinfo
  drwx             Tue Jan  1 00:00:32 2019   hotspot

ap505-13403B#
```

re-elect

Re-elects the tunnel controller (wireless controller or service platform)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> • on <DEVICE-NAME> – Optional. Re-elects the tunnel controller on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Initiates device(s) reload and configures associated parameters The following keyword is recursive and allows you to specify multiple devices: • <DEVICE-MAC-OR-HOSTNAME> – Optional. Reloads a specified device(s), identified by the <DEVICE-MAC-OR-HOSTNAME> keyword. Specify the device's hostname or MAC address. **Note:** If no device is specified, the system reloads the logged device.

```
reload {at <TIME> <1-31> <MONTH> <1993-2035> {on <DEVICE-OR-DOMAIN-NAME>}}
```

reload at	Initiates device(s) reload and configures associated parameters • at – Optional. Schedules a reload at a specified time and day. Use the following keywords to specify the time and day: <TIME>, <1-31>, <MONTH>, and <1993-2035>.
<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>	Optional. Performs reload at the scheduled time, on a specified device or all devices within a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – 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.

```
reload {cancel} {on <DEVICE-OR-DOMAIN-NAME>}
```

reload cancel on <DEVICE-OR-DOMAIN-NAME>	Cancels pending/scheduled reloads of device(s) cancel – Optional. Cancels all pending reloads • on <DEVICE-OR-DOMAIN-NAME> – Optional. Cancels reloads pending on a specified device or all devices within a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain. Note: If no device is specified, the system cancels reloads pending on the logged device.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Reloads on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
reload {force} {(<DEVICE-MAC-OR-HOSTNAME>)}
```

reload force	Initiates device(s) reload and configures associated parameters • 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.
<DEVICE-MAC-OR-HOSTNAME>	This keyword is recursive and allows you to specify multiple devices. • <DEVICE-MAC-OR-HOSTNAME> – Optional. Forces a reload on a specified device identified by the <DEVICE-MAC-OR-HOSTNAME> 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. Note: If no device is specified, the system forcefully reloads the logged device.

```
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	Initiates device(s) reload and configures associated parameters • 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.
on <DOMAIN-NAME> staggered	Optional. Forces a reload on all devices in a RF Domain • <DOMAIN-NAME> – 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. • 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.

staggered {<DEVICE-MAC-OR-HOSTNAME>| on <DOMAIN-NAME>}	Optional. Enables staggered reload of devices (one at a time) without network impact • <DEVICE-MAC-OR-HOSTNAME> – Optional. Forces a reload on specified device(s) identified by the <DEVICE-MAC-OR-HOSTNAME> 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. • on <DOMAIN-NAME> – 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. Note: If no device or RF Domain is specified, the system forcefully reloads the logged device.

{containing <WORD>| exclude-controllers exclude-rf-domain-manager| filter <DEVICE-TYPE>}	When forcefully reloading devices in a RF Domain, you can use following options to filter specific devices or device types:
	• containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames
	  • <WORD> – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and forcefully reloaded.
	• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process
	• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process
	• filter <DEVICE-TYPE> – 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.
	  • <DEVICE-TYPE> – Select the type of device to reload. The options are: AP505, AP510, AP560, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533, NX5500, NX75XX, NX9000, NX9600, VX9000.

```
reload {in <1-999>} {list {<LINE>|all}|on <DEVICE-OR-DOMAIN-NAME>}
```

reload in <1-999>	Initiates device(s) reload and configures associated parameters • in – Optional. Performs a reload after a specified time period • <1-999> – Specify the time from 1 - 999 minutes
list {<LINE>|all}	Optional. Reloads all adopted devices or specified devices • <LINE> – Optional. Reloads listed devices. List all devices (to be reloaded) separated by a space. • all – Optional. Reloads all devices adopted by this controller
on <DEVICE-OR-DOMAIN-NAME>	Optional. Reloads a specified device or all devices within a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
reload {on <DOMAIN-NAME>} {containing <WORD>|exclude-controllers|
exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

reload on <DOMAIN-NAME>	Initiates device(s) reload and configures associated parameters
	• on <DOMAIN-NAME> – Optional. Enables reload of all devices in a RF Domain
	  • <DOMAIN-NAME> – 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.
	
	  Note: If no RF Domain is specified, the system reloads the logged device.

{containing <WORD>| exclude-controllers| exclude-rf-domain-manager| filter <DEVICE-TYPE>}	When reloading devices in a RF Domain, you can use following options to filter specific devices or device types:
	• containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames.
	  • <WORD> – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and forcefully reloaded.
	• exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process
	• exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process
	• filter <DEVICE-TYPE> – 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.
	  • <DEVICE-TYPE> – Select the type of device to reload. The options are: AP505, AP510, AP560, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533, NX5500, NX75XX, NX9000, NX9600, VX9000.

```
reload {staggered} {(<DEVICE-MAC-OR-HOSTNAME>)|on <DOMAIN-NAME>} {containing <WORD>|
exclude-controllers|exclude-rf-domain-manager|filter <DEVICE-TYPE>}
```

reload staggered	Initiates device(s) reload and configures associated parameters • staggered – Optional. Enables staggered reload of devices (one at a time) without network impact
{<DEVICE-MAC-OR-HOSTNAME>| on <DOMAIN-NAME>}	Use one of the following options to specify a single device, multiple devices, or a RF Domain • <DEVICE-MAC-OR-HOSTNAME> – Optional. Performs staggered reload on specified device(s) identified by the <DEVICE-MAC-OR-HOSTNAME> 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. • <DOMAIN-NAME> – 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. Note: If no device or RF Domain is specified, the system reloads the logged device.
{containing <WORD>| exclude-controllers| exclude-rf-domain-manager| filter <DEVICE-TYPE>}	When reloading devices in a RF Domain, you can use following options to filter specific devices or device types: • containing <WORD> – Optional. Filters out devices containing a specified sub-string in their hostnames. • <WORD> – Optional. Provide the sub-string to match. All devices having hostnames containing the provided sub-string are filtered and reloaded. • exclude-controllers – Optional. Excludes all controllers in the specified RF Domain from the reload process • exclude-rf-domain-manager – Optional. Excludes the RF Domain manager from the reload process • filter <DEVICE-TYPE> – 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. <DEVICE-TYPE> – Select the type of device to reload. The options are: AP505, AP510, AP560, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533, NX5500, NX75XX, NX9000, NX9600, VX9000.

Example

```
ap510-133B38#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       06/28/2019 02:43:33     07/02/2019 13:28:20     7.2.0.0-009D
  Secondary     06/21/2019 02:34:38     06/25/2019 14:46:00     7.2.0.0-006D
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Primary
Software Fallback  : Enabled
ap510-133B38#

ap510-133B38#reload
The system will be rebooted, do you want to continue? (y/n): y
```

```
Save current configuration? ([y]es/[n]o/[d]isplay unsaved/[c]ancel reload): y
[OK]
ap510-133B38#
ap510-133B38#show boot
------------------------------------------------------------------------------------
     IMAGE            BUILD DATE              INSTALL DATE          VERSION
------------------------------------------------------------------------------------
  Primary       06/28/2019 02:43:33     07/02/2019 13:28:20     7.2.0.0-009D
  Secondary     06/21/2019 02:34:38     06/25/2019 14:46:00     7.2.0.0-006D
------------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
ap510-133B38#
```

rename

Renames a file in the devices' file system

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
nx9500-6C8809#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

nx9500-6C8809#
nx9500-6C8809#rmdir Final
nx9500-6C8809#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

nx9500-6C8809#
```

self

Enters the logged device's configuration context

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

t5

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 on page 120.

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Copies file to an external server • <SOURCE-FILE-NAME> – Specify the source file name. • <DEST-FILE-NAME> – Specify the destination file name. The content from the source file is copied to the destination file. 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.
delete <FILE-NAME>	Deletes files on the T5 device's file system • <FILE-NAME> – Specify the file name. The specified file is deleted.
rename <SOURCE-FILE-NAME> <DEST-FILE-NAME>	Renames a file on the T5 device's file system • <SOURCE-FILE-NAME> – Specify the source file name • <DEST-FILE-NAME> – Specify the new file name. The source file is renamed to the input provided here.
write memory	Writes running configuration to an adopted T5 device's memory • memory – Writes running configuration to the T5 device's *non-volatile* (NV) memory.
on <T5-DEVICE-NAME>	Optional. Executes these operation on a specified T5 device • <T5-DEVICE-NAME> – Specify the T5 device's hostname.

Example

```
nx9500-6C8809#t5 write memory on t5-ED7C6C
Success
nx9500-6C8809#
```

upgrade

Upgrades a device's software image

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 one of the following format: cf:/path/file usb1:/path/file usb2:/path/file usb<n>:/path/file

<URL>	Specify the target firmware image location. Use one of the following formats:
	• IPv4 URLS:
	  • 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:
	  • 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

background	Optional. Performs upgrade in the background
on <DEVICE-NAME>	Optional. Upgrades the software image on a specified remote device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <RF-DOMAIN-NAME>	Optional. Upgrades the software image on all devices within a specified RF Domain • <RF-DOMAIN-NAME> – Specify the name of the RF Domain.

```
upgrade dhcp-vendor-options {<DEVICE-NAME>} {<DEVICE-NAME>}
```

dhcp-vendor-options	Uses DHCP vendor options to upgrade device(s)
<DEVICE-NAME> {<DEVICE-NAME>}	Optional. Uses DHCP vendor options to upgrade a specified device. Specify the name of the AP, wireless controller, or service platform. • <DEVICE-NAME> – Optional. You can optionally specify multiple comma-separated device names/MAC addresses to upgrade.

```
upgrade dhcp-vendor-options {on <RF-DOMAIN-NAME>} {containing <SUB-STRING>|
exclude-controllers|exclude-rf-domain-managers|filter <DEVICE-TYPE>}
```

dhcp-vendor-options	Uses DHCP vendor options to upgrade device(s)

on <RF-DOMAIN-NAME> {containing <SUB-STRING>| exclude-controllers| exclude-rf-domain-managers| filter <DEVICE-TYPE>}	Optional. Uses DHCP vendor options to upgrade all devices or specified device(s) within the RF Domain identified by the <RF-DOMAIN-NAME> keyword
	• <RF-DOMAIN-NAME> – 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:
	  • containing <SUB-STRING> – Optional. Upgrades all devices, within the specified RF Domain, containing a specified sub-string in their hostname
	  <SUB-STRING> – Specify the sub-string to match.
	• 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.
	• 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.
	• filter <DEVICE-TYPE> – Optional. Executes the command on all devices, within the specified RF Domain, of a specified type
	  • <DEVICE-TYPE> – Specify the device type. The options are: AP505, AP510, AP560, NX5500, NX7500, NX9500, NX9600, and VX9000. Upgrades all devices of the type specified here. For example, if AP510 is the device-type specified, all AP510 within the specified RF Domain are upgraded.

Example

```
nx9500-6C8809#upgrade ftp://symbol:symbol@134.141.244.24/NX9500-7.2.0.0-006D.img

Running from partition /dev/sda8
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 7.2.0.0-006D
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
------------------------------------------------------------------------------------
  Primary       06/21/2019 04:10:19     06/25/2019 14:01:30     7.2.0.0-006D
  Secondary     05/25/2019 07:14:53     06/03/2019 14:11:03     5.9.5.0-004D
------------------------------------------------------------------------------------
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.

```
nx9500-6C8809#reload
The system will be rebooted, do you want to continue? (y/n): y
nx9500-6C8809#
```

The following example shows the upgrade status:

```
nx9500-6C8809#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 2019-06-25 14:01:30
-----------------------------------------------
Running from partition /dev/sda8
var2 is 0 percent full
/tmp is 3 percent full
Free Memory 34871840 kB
FWU invoked via Linux shell
Validating image file header
Removing other partition
Mon Jun  3 14:27:05 UTC 2019
debug: cmdline -C /boot/lilo.conf -R 5.9.5.0-004D -P fix
LILO version 22.6-CCB, Copyright (C) 1992-1998 Werner Almesberger
Development beyond version 21 Copyright (C) 1999-2004 John Coffman
Released 02-Sep-2004, and compiled at TIME on DATE

Tue Jun 18 14:45:09 UTC 2019
debug: cmdline -C /boot/lilo.conf -P fix
LILO version 22.6-CCB, Copyright (C) 1992-1998 Werner Almesberger
Development beyond version 21 Copyright (C) 1999-2004 John Coffman
Released 02-Sep-2004, and compiled at TIME on DATE

Reading boot sector from /dev/sda
--More--

nx9500-6C8809#
```

```
nx9500-6C8809#show adoption status
-------------------------------------------------------------------------------------------------
--------------------
DEVICE-NAME    VERSION     CFG-STAT       MSGS  ADOPTED-BY   LAST-ADOPTION   UPTIME
IPv4-ADDRESS
-------------------------------------------------------------------------------------------------
--------------------
ap505-134038 7.1.2.0-013R version-mismatch No  nx9500-6C8809 0 days 00:07:33 26 days
02:13:49  10.234.160.36
-------------------------------------------------------------------------------------------------
```

```
--------------------
Total number of devices displayed: 4
nx9500-6C8809#
nx9500-6C8809#device-upgrade ap505-134038
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
-------------------------------------------------------------------------------
  B4-C7-99-6C-88-09         Success         Queued 1 devices to upgrade
-------------------------------------------------------------------------------
nx9500-6C8809#
```

Related Commands

no on page 160	Removes a patch installed on a specified device

upgrade-abort

Aborts an ongoing software image upgrade

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Examples

```
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.3.0-010D.img
Running from partition /dev/mtdblock6
Validating image file header
Making file system
Extracting files (this may take some time)..................
rfs4000-6DB5D4#upgrade-abort
rfs4000-229D58#upgrade ftp://anonymous:anonymous@192.168.13.10/LatestBuilds/W59/
RFS4000-5.9.3.0-010D.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#
```

raid

Enables RAID *(Redundant Array of Independent Disks)* 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)

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.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

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. 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 **Note:** When enabled, an audible alarm is triggered when a drive in the array fails. The silence command deactivates the alarm (sound). **Note:** To enable RAID alarm, in the device configuration mode, use the `raid > alarm > enable` command. An NX 9500 profile can also have the RAID alarm feature activated. For more information on the enabling RAID alarm, see raid on page 1301.

```
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. **Note:** 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. **Note:** 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. **Note:** Blinking LEDs enable you correctly locate a drive.
remove <0-4>	Removes (shuts downs) a disk from the array, before it is physically removed from its slot. Specify the drive number containing the disk. **Note:** 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#
```

no

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [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 NX9500 and NX9600 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#
```

5 Global Configuration Commands

global-config-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
  ap505                               AP505 access point
  ap510                               AP510 access point
  ap560                               AP560 access point
  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
ble-data-export-policy                Configure a ble data export  policy
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
iot-device-type-imagotag-policy       Configure a iot imagotag device type
                                      policy
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
location-policy                       Configure a location policy used for
                                      ExtremeLocation
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
  purview-application-group         Configure a Purview application-grou
  purview-application-policy        Configure a Purview application policy
  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
aaa-policy on page 170	Creates a *AAA (Authentication, Authorization, and Accounting)* policy and enters its configuration mode. This policy enables administrators to define access control within the network.
aaa-tacacs-policy on page 171	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.
alias on page 172	Configures network, VLAN, and service aliases
ap505 on page 182	Adds an AP505 to the network
ap510 on page 182	Adds an AP510 to the network
application on page 183	Creates an application definition and enters its configuration mode. This command allows you to create a customized application detection definition.
application-group on page 191	Creates an application group and enters its configuration mode
application-policy on page 195	Creates an application policy and enters its configuration mode. This policy defines the actions executed on recognized HTTP (for example, Facebook), enterprise (for example, Webex) and peer-to-peer (for example, gaming) applications or application-categories.
association-acl-policy on page 212	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.
auto-provisioning-policy on page 213	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.
bgp on page 214	Configures *BGP (Border Gateway Protocol)* settings
ble-data-export-policy on page 216	Creates a *Bluetooth Low Energy* (BLE) data export policy and enters its configuration mode.
bonjour-gw-discovery-policy on page 219	Creates a *Bonjour* GW Discovery policy and enters its configuration mode. This policy configures the VLANs on which Bonjour services are located.
bonjour-gw-forwarding-policy on page 223	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.
bonjour-gw-query-forwarding-policy on page 224	Creates a Bonjour GW Query Forwarding policy and enters its configuration mode. This policy enables Bonjour query forwarding across multiple VLANs.
captive-portal on page 225	Creates a captive portal and enters its configuration mode
clear on page 270	Clears the event history
client-identity on page 271	Creates a client identity definition and enters its configuration mode. This feature enables client identification through DHCP device fingerprinting.
client-identity-group on page 277	Creates a new client identity group and enters its configuration mode

Table 6: Global Config Commands (continued)

Command	Description
clone on page 281	Clones a specified configuration object
crypto-cmp-policy on page 282	Creates a *Certificate Management Protocol* (CMP) policy and enters its configuration mode. CMP is an Internet protocol designed to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network.
customize on page 283	Customizes the CLI command summary output
database-client-policy global-config on page 296	Creates a database client policy and enters its configuration mode. In case of ExtremeWireless WiNG deployments integrated with Extreme Nsight and ExtremeGuest, use this option to configure the credentials required to authenticate with the Extreme Nsight or ExtremeGuest server database.
database-policy global config on page 299	Creates a database policy and enters its configuration mode. This policy enables the database, and also configures the database replica set.
device on page 304	Specifies configuration on multiple devices
device-categorization on page 305	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.
dhcp-server-policy on page 308	Creates a *DHCP (Dynamic Host Configuration Protocol)* 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.
dhcpv6-server-policy on page 309	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.
dns-whitelist on page 310	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.
event-system-policy on page 351	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.
ex3500 on page 313	Creates an EX3500 time range list and enters its configuration mode
ex3500-management-policy on page 317	Creates an EX3500 management policy and enters its configuration mode. This policy controls access to the EX3500 switch from management stations using SNMP.
ex3500-qos-class-map-policy on page 333	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, prevents EX3500 switch bandwidth congestion, and prevents packet drops.
ex3500-qos-policy-map on page 338	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.
ex3524 on page 348	Adds a EX3524 switch to the network
ex3548 on page 350	Adds a EX3548 switch to the network

Table 6: Global Config Commands (continued)

Command	Description
firewall-policy on page 366	Creates a firewall policy and enters its configuration mode. This policy configures safe guards against *DoS* attacks and packet storms. It also configures firewall parameters, such as logging, application layer gateway, TCP protocol checks, state flow checks, etc.
global-association-list on page 367	Configures a global list of client MAC addresses
guest-management-policy on page 370	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 *Service Set Identifier* (SSID).
host on page 380	Sets the system's network name
inline-password-encryption on page 381	Stores the encryption key in the startup configuration file
iot-device-type-imagotag-policy on page 381	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).
ip on page 390	Creates a IP *ACL (Access Control List)* and/or a *SNMP (Simple Network Management Protocol)* ACL, and enters its configuration mode
ipv6 on page 392	Creates a IPv6 ACL and enters its configuration mode
ipv6-router-advertisement-policy on page 393	Creates an IPv6 *router advertisement* (RA) policy and enters its configuration mode
l2tpv3 on page 404	Configures *Layer 2 Tunneling Protocol Version 3* (L2TPv3) tunnel policy and enters its configuration mode. This policy defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.
location-policy on page 406	Configures a location policy and enters its configuration mode
mac on page 410	Configures *MAC* access lists (goes to the MAC ACL mode)
management-policy on page 411	Creates a management policy and enters its configuration context. This policy configures services that run on a device, such as welcome messages, banners, etc.
meshpoint on page 412	Creates a meshpoint and enters its configuration mode
meshpoint-qos-policy on page 413	Creates a meshpoint *QoS (Quality of Service)* policy and enters its configuration mode
mint-policy on page 414	Creates a MiNT security policy and enters its configuration mode
nac-list on page 415	Creates a network ACL and enters its configuration mode
no on page 611	Negates a command or sets its default
nsight-policy (global-config-mode) on page 418	Creates an NSight policy and enters its configuration mode
passpoint-policy on page 426	Creates a new passpoint policy and enters its configuration mode
password-encryption on page 427	Enables password encryption
profile on page 428	Creates a device profile and enters its configuration mode
purview-application-group on page 432	Creates a Purview Application Group and enters its configuration mode

Table 6: Global Config Commands (continued)

Command	Description
purview-application-policy on page 436	Creates a Purview Application Policy and enters its configuration mode
radio-qos-policy on page 453	Creates a radio *QoS* policy and enters its configuration mode
radius-group on page 454	Creates a *RADIUS (Remote Authentication Dial In User Service)* group and enters its configuration mode
radius-server-policy on page 455	Creates a RADIUS server policy and enters its configuration mode
radius-user-pool-policy on page 456	Creates a RADIUS user pool policy and enters its configuration mode
rename on page 457	Renames and existing *top-level object* (TLO)
replace on page 458	Selects an existing device by its MAC address or hostname and replaces it with a new device having a different MAC address
rf-domain on page 460	Creates an RF Domain and enters its configuration mode
roaming-assist-policy on page 493	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.
nx5500 on page 491	Adds an NX5500 to the network
nx7500 on page 491	Adds an NX7500 to the network
nx9000 on page 492	Adds an NX9500 to the network
role-policy on page 494	Creates a role policy and enters its configuration mode
route-map on page 495	Creates a dynamic BGP route map and enters its configuration mode
routing-policy on page 496	Creates a routing policy and enters its configuration mode
rtl-server-policy on page 496	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.
schedule-policy on page 499	Creates a schedule policy and enters its configuration mode
self on page 503	Displays a logged device's configuration context
sensor-policy on page 503	Creates a sensor policy and enters its configuration mode
smart-rf-policy on page 508	Creates a Smart RF policy and enters its configuration mode
t5 on page 509	Configures a t5 wireless controller. This command is applicable only on the RFS4010, NX7500, NX9500, NX9600, and VX9000 platforms.
web-filter-policy on page 511	Creates a Web Filtering policy and enters its configuration mode
wips-policy on page 517	Creates a WIPS policy and enters its configuration mode
wlan on page 518	Creates a *WLAN (Wireless Local Area Network)* and enters its configuration mode
wlan-qos-policy on page 593	Creates a WLAN QoS policy and enters its configuration mode
url-filter on page 594	Creates an URL filter and enters its configuration mode. URL filtering is a licensed feature.

Table 6: Global Config Commands (continued)

Command	Description
url-list on page 604	Creates an URL list and enters its configuration mode.
vx9000 on page 608	Configures a *Virtual WLAN Controller* (V-WLC) in a *virtual machine* (VM) environment

Note
For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Common Commands on page 616.

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. AAA policies 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing AAA policy

Note
For more information on the AAA policy commands, see AAA Policy on page 1303.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing AAA TACACS policy

Note
For more information on the AAA-TACACS policy commands, see AAA-TACACS Policy on page 1763.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|igp|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 <ADRESS-RANGE-ALIAS-NAME>	Creates an address range alias, defining a range of IP addresses • <ADRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. Note: Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range.

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
```

encrypted-string <ENCRYPTED-STRING-ALIAS-NAME>	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 snmp-server on page 1539 (management policy config mode). • <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name. Note: Alias name should begin with '$'.

[0|2] <LINE>	Configures the value associated with the alias name specified in the previous step
	• [0|2] <LINE> – Configures the alias value
	
	Note: If password-encryption is enabled, in the `show > running-config` output, this clear text is displayed as an encrypted string, as shown below:
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`alias encrypted-string $enString 2`
	`fABMK2is7UToNiZE3MQXbgAAAAxB0ZIysdqsEJwr6AH/Da//`
	`!`
	`--More--`
	`nx9500-6C8809`
	
	In the above `show > running-config` 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:
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`!`
	`alias encrypted-string $enString 0 test11223344`
	`!`
	`--More--`
	`nx9500-6C8809`
	
	For more information on enabling password-encryption, see password-encryption on page 427.

```
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/l/BXm9c4SBDv`
	`!`
	`alias hashed-string $PriMode 1`
	`faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112e`
	`cfc75`
	`0`
	`--More--`
	`nx9500-6C8809`
	In the above `show > running-config` output, the '1' 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>	Creates a network-group alias • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Note: Alias name should begin with '$'. 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. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.
host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the hosts' IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.

```
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)}
```

alias network-service <NETWORK-SERVICE-ALIAS-NAME>	Configures an alias that specifies available network services and the corresponding source and destination software ports • <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. Note: Alias name should begin with '$'. 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.
proto [<0-254>| <WORD>|eigrp|gre| igmp|igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – 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. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects EIGRP *(Enhanced Interior Gateway Routing Protocol)*. The protocol number 88. • gre – Selects GRE *(Generic Routing Encapsulation)*. The protocol number is 47. • igmp – Selects IGMP *(Internet Group Management Protocol)*. The protocol number is 2. • igp – Selects IGP *(Interior Gateway Protocol)*. The protocol number is 9. • ospf – Selects OSPF *(Open Shortest Path First)*. The protocol number is 89. • vrrp – Selects VRRP *(Virtual Router Redundancy Protocol)*. The protocol number is 112.
{(<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)}	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. • <1-65535> – Optional. Configures a destination port number from 1 - 65535 • <WORD> – Optional. Identifies the destination port by the service name provided. For example, the SSH service uses TCP port 22. • bgp – Optional. Configures the default BGP *(Border Gateway Protocol)* services port (179) • dns – Optional. Configures the default DNS *(Domain Name System)* services port (53) • ftp – Optional. Configures the default FTP *(File Transfer Protocol)* control services port (21) • ftp-data – Optional. Configures the default FTP data services port (20) • gopher – Optional. Configures the default gopher services port (70) • https – Optional. Configures the default HTTPS services port (443) • ldap – Optional. Configures the default LDAP *(Lightweight Directory Access Protocol)* services port (389) • nntp – Optional. Configures the default NNTP *(Newsgroup)* 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 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>
```

alias string <STRING-ALIAS-NAME>	Creates a string alias identified by the <STRING-ALIAS-NAME> keyword • <STRING-ALIAS-NAME> – Specify the string alias name. **Note:** Alias name should begin with '$'. • <LINE> – Specify the string value. 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* • the string value it is mapped to is: *test.example_company.com* (a domain name). 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 bonjour-gw-discovery-policy on page 219.

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

alias vlan <VLAN-ALIAS-NAME>	Creates a VLAN alias identified by the <VLAN-ALIAS-NAME> keyword • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. **Note:** Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094.

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/
QAAAAgc0l8ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
vnx9500-6C8809(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/
```

```
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)#
```

Related Commands

no on page 611	Removes an existing network, VLAN, service, or string alias

ap505

Invokes an AP505 acces point's configuration context.

Supported in the following platforms:

- Access Point — AP505
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ap505 <MAC>
```

Parameters

```
ap505 <MAC>
```

<MAC>	Specify the AP505's MAC address.

Examples

```
nx9500-6C8809(config)#ap505 2B-16-0c-18-0D-11
nx9500-6C8809(config-device-2B-16-0c-18-0D-11)#show con
ap505 2B-16-0c-18-0D-11
 use profile default-ap505
 use rf-domain default
 hostname ap505-180D11
nx9500-6C8809(config-device-2B-16-0c-18-0D-11)#
```

Related Commands

no on page 611	Removes an AP510 from the network

ap510

Invokes an AP510 acces point's configuration context.

Supported in the following platforms:

- Access Point — AP510
- Wireless Controllers — RFS4000

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ap510 <MAC>
```

Parameters

```
ap510 <MAC>
```

<MAC>	Specify the AP510's MAC address.

Examples

```
nx9500-6C8809(config)#ap510 01-11-CD-21-0B-13
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#show con
ap510 01-11-CD-21-0B-13
 use profile default-ap510
 use rf-domain default
 hostname ap510-210B13
nx9500-6C8809(config-device-01-11-CD-21-0B-13)#
```

Related Commands

no on page 611	Removes an AP510 from the network

application

Global Configuration Commands on page 163

Creates an application definition and enters its configuration mode. Use this command to create application detection signatures that are not in the pre-defined set of application definitions provided by ExtremeWireless WiNG.

Application Visibility and Control (AVC) enables detection of top-level hosting applications along with the services these applications host. It also provides Metadata extraction capabilities for a variety of protocols and applications.

AVC and statistics reporting is available on both the WiNG 5.9.X and WiNG 7.1.X operating systems. However, the DPI engine used to check the data points varies. The WiNG 7.1.X OS uses *EAA (Extreme Application Analytics)* (Purview™) DPI engine to detect applications (layer 7 traffic) and manage traffic flow. It recognizes 36 application categories with 2457 applications. The WiNG 5.9.X operating system uses a third-party DPI engine, which recognizes 23 application-categories with a total of 2384 applications.

The `application` command is part of the AVC feature. It allows you to create custom application definitions to detect native applications. Refer to the following on how to use the customized application definitions:

- For WiNG 5.9.X networks, configure the application definition on the controller and apply in the following contexts.
  - To enable packet filtering on WiNG 5.9.X APs, use the application definition in the application-policy on page 195 and specify allow, deny or mark rules for these application packets.

- To enable mandatory stats reporting on WiNG 5.9.X APs, use the application definition in an application-group on page 191.

- For WiNG 7.1.2 networks, configure the application definition on the controller and apply in the following contexts:
  - To enable packet filtering on WiNG 7.1.X APs, use the application definition in the purview-application-policy on page 436 and specify allow, deny or mark rules for these application packets .
  - To enable packet filtering on WiNG 7.1.X APs, use the custom application definition in an purview-application-group on page 432.

Note
The WiNG 7.1.2 OS does not support Purview™ on NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Supported on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
application <APPLICATION-NAME>
```

Parameters

```
application <APPLICATION-NAME>
```

application <APPLICATION-NAME>	Creates a new application definition and enters its configuration mode • <APPLICATION-NAME> – Specify a name of the new application definition. It is created if not already existing in the system.

Examples

```
nx9500-6C8809(config-application-Custom)#?
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
  purview-app-category  Set application category (default is custom)
  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-Custom)#
```

Related Commands

no on page 611 (global-config-mode)	Removes an existing application definition
app-category on page 185	Configures the application category type for the custom application definition Note: In WiNG 5.9.X deployments, use this parameter to define the app-category of the custom application definition.
purview-app-category on page 188	Configures the application category type for the custom purview-application definition Note: In WiNG 7.1.2 deployments, use this parameter to define the purview-app-category type of the custom application definition.
application-group on page 191	Creates an application group and enters its configuration mode.
application-policy on page 195	Creates an application policy and enters its configuration mode.
purview-application-group on page 432	Creates a Purview application group and enters its configuration mode.
purview-application-policy on page 436	Creates a Purview application policy and enters its configuration mode.

app-category

application on page 183

Configures the application category type for this custom application definition.

Note
This parameter is applicable only for WiNG 5.9.X supported APs. Define the app-category type for this custom application definition. Use this custom application definition in the application-group on page 191 and application-policy on page 195 contexts.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Note
This parameter is not applicable for the WiNG 7.1.2 AP5XX model APs.

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. 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 custom
nx9500-6C8809(config-application-Bing)#show context
application Bing
 app-category streaming
nx9500-6C8809(config-application-Bing)#
```

Related Commands

no on page 190	Resets application category to default (custom)

description

application on page 183

Configures a description for this application definition

Supported on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this application definition • <WORD> – Specify a description not exceeding 80 characters in length. Enter the descriptive text within double quotes.

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

no on page 190	Removes this description configured for this application

https

application on page 183

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 on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

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: • contains – Filters applications having common-name attributes containing the string specified here • ends-with – Filters applications ending with the string specified here • <WORD> – Specify the string to match (should not exceed 64 characters).

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

no on page 190	Removes the HTTPS common-name attribute value configured with this application category

purview-app-category

application on page 183

Configures the application category type for this custom (user-defined) purview-application definition

Note

This parameter is applicable only for WiNG 7.1.2 supported APs. Define the purview-app-category type of this custom application definition. Apply this custom application definition in the purview-application-group on page 432 and purview-application-policy on page 436 contexts.

Supported on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

Syntax

```
purview-app-category <PURVIEW-APP-CATEGORY-NAME>
```

Parameters

```
purview-app-category <PURVIEW-APP-CATEGORY-NAME>
```

purview-app-category <PURVIEW-APP-CATEGORY-NAME>	Select the category best suited for this application definition. The *EAA*, formerly known as Purview™, supports 36 application categories with 2457 applications. Note: Refer to Examples below for the app-categories supported by the Purview™ engine. 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-Custom)#purview-app-category
ads               biz               certs             cloud
cloudcpu          corp              custom            db
education         finance           games             health
location          mail              news              other
p2p               proto             realtimecomms     restrictcontent
search            shopping          social            sports
storage           streaming         travel            unknown
updates           vpn               webapp            webcontent
webfile           webmeet
nx9500-6C8809(config-application-Custom)#
```

The following example displays the canned (built-in, system-provided apps) starting with 'h':

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application h [TAB]
hashforcash  hashunited  hoopla
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
```

The following example, creates application definition 'hulu' and assigns it to the app-category 'streaming'.

```
nx9500-6C8809(config)#application hulu
nx9500-6C8809(config-application-hulu)#
nx9500-6C8809(config-application-hulu)#purview-app-category streaming
```

```
nx9500-6C8809(config-application-hulu)#show context
application hulu
 purview-app-category streaming
nx9500-6C8809(config-application-hulu)#
```

The following example shows 'hulu' application definition added to the list of available applications:

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application h [TAB]
hashforcash  hashunited   hoopla hulu
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
```

Related Commands

no on page 190	Resets application category to default (custom)

use

application on page 183

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 on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

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 • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). The network-service alias should specify the protocols and ports to match.
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. • <URL-LIST-NAME> – Specify the URL list name (should be existing and configured). The URL list should specify the HTTP URL host names to match.

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 on page 190	Removes the network-service alias or the URL list associated with this application definition

no

application on page 183

Removes or resets this application definition's configured settings

Supported on the following WiNG 7.1.2 APs:

- Access Points — AP505i, AP510i/e, AP560i/h

Syntax

```
no [app-category|description|https|purview-app-category|use]
```

Note
The 'purview-app-category' parameter is applicable only on the WiNG 7.1.X, AP5XX model APs.

```
no [app-category|purview-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

Examples

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
nx9500-6C8809(config-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

Global Configuration Commands on page 163

Creates an Application Group and enters its configuration mode. An application group is a collection of system-provided and/or user-defined applications. Application group allows you to enforce mandatory stats reporting for specific traffic types.

The WiNG 5.9.X OS uses a third-party DPI engine to implement *Application Visibility and Control* (AVC). It detects top-level hosting applications (layer 7) along with the services these applications host.

Use AVC to implement:

- Packet filtering - allow, deny or mark packets based on rules defined in the Application policy.
- Mandatory stats reporting - enable mandatory stats reporting for an application or set of applications defined in the Application group.

The `application-group` command is part of the mandatory stats reporting feature. To enable mandatory stats reporting, follow the steps below:

1 Create an application-group and specify the applications for which mandatory stats reporting is to be enabled.

Note
If the required application definition is not system-provided, use the `application` command to create a custom app signature.

2 Use this application-group in the NSight policy.

3 Apply the NSight policy in the RF Domain context.

Note
For more information and examples, see mandatory on page 420.

Note
For information on enabling mandatory stats reporting on WiNG 7.1.2 APs see `purview-application-group`.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
application-group <APPLICATION-GROUP-NAME>
```

Parameters

```
application-group <APPLICATION-GROUP-NAME>
```

application-group <APPLICATION-GROUP-NAME>	Creates an application group and enters its configuration mode • <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.

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 on page 611 (global-config-mode)	Removes an existing application group
application-policy on page 195	Creates an application policy and enters its configuration mode.
application on page 183	Creates an application definition and enters its configuration mode. Use this command to create customized application detection signatures.

application

application-group on page 191

Adds an application to this application group. You can add a system-provided or user-defined application.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 on page 183 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 on page 194	Removes a specified application from this application group

description

application-group on page 191

Configures a description for this application group

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this application group that uniquely differentiates it from other existing application groups • <WORD> – Provide a description not exceeding 80 characters in length.

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 on page 194	Removes the description configured for this application group

no

application-group on page 191

Removes this application group's configured parameters (application and/or description)

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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

Global Configuration Commands on page 163

Creates an application policy and enters its configuration mode. Application policies allow you to define rules that dictate how each traffic type is managed on your network. An application policy contains application (Layer 7) rules.

An application rule leverages the AP's *deep packet inspection* (DPI) engine to detect the underlying application to which a frame or flow belongs. The rule then applies access control and quality of service actions to all the traffic associated with the application, not just traffic destined for specific IP addresses or ports. The control actions regulate both access control and traffic engineering (rate limit, marking, and prioritization) for applications and groups.

Once created and configured, apply the application policy at the following levels within the network to enforce application assurance:

- RADIUS *change of authorization* (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.

Note
The WiNG 7.1.2 enabled, AP5XX model access points implement application visibility and control through the purview-application-policy on page 436.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
application-policy <APPLICATION-POLICY-NAME>
```

Parameters

```
application-policy <APPLICATION-POLICY-NAME>
```

application-policy <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 on page 611 (global-config-mode)	Removes an existing application policy
application on page 183	Creates an application definition and enters its configuration mode. Use this command to create customized application detection signatures.
application-group on page 191	Creates an application group and enters its configuration mode.

allow

application-policy on page 195

Creates an allow rule and configures the match criteria based on which packets are filtered and the allow access action applied

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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]	Uses application category as the match criteria • <APP-CATEGORY-NAME> – 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. • all – The system forwards all packets irrespective of the application category.
application <APPLICATION-NAME>	Uses application name as the match criteria • <APPLICATION-NAME> – 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. Note: The WiNG system provides approximately 309 canned applications. In addition to these, the database also includes custom-made applications. These are application definitions created using the application on page 183 command.

schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this allow rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – 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 > 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. **Note:** 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 enforcement-time on page 203.

precedence <1-256>	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.
	Let us consider application *youtube* belonging to app-category *streaming*. The action required is: Allow youtube packets, and deny all other applications belonging to app-category streaming.
	The rules can be defined as:
	`#allow application youtube precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application youtube precedence 2`
	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.
	The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

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

no on page 211	Removes this allow rule from the application policy

deny (application-policy-config-mode)

application-policy on page 195

Creates a deny rule and configures the match criteria based on which packets are filtered and the deny access action applied

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 • <APP-CATEGORY-NAME> – 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. • all – The system drops all packets irrespective of the application category.
application <APPLICATION-NAME>	Uses application name as the match criteria • <APPLICATION-NAME> – 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. 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.

schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this deny rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – 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 > 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time on page 203.

precedence <1-256>	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 *youtube* belonging to app-category *streaming*. The rules can be defined as:
	`#allow application youtube precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application youtube precedence 2`
	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.
	The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

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

no on page 211	Removes this deny rule from the application policy

description

application-policy on page 195

Configures a brief description for this application policy that enables you to differentiate it from other application policies

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
description <LINE>
```

Parameters

```
description <LINE>
```

description <LINE>	Configures this application policy's description • <LINE> – Specify a brief description not exceeding 80 characters in length.

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 on page 211	Removes this application policy's description

enforcement-time

application-policy on page 195

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 on page 499.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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	Enforces this application policy on only on the days specified here • sunday – Enforces the policy only on Sundays • monday – Enforces the policy only on Mondays • tuesday – Enforces the policy only on Tuesdays • wednesday – Enforces the policy only on Wednesdays • thursday – Enforces the policy only on Thursdays • friday – Enforces the policy only on Fridays • saturday – Enforces the policy only on Saturdays • all – Enforces the policy on all days. This is the default setting. • weekends – Enforces the policy only on weekends • weekdays – Enforces the policy only on weekdays In case no enforcement time is specified, the application policy is enforced on all days (i.e., always active). 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').
start-time <HH:MM> end-time <HH:MM>	Optional. Configures this application policy's enforcement period • start-time – Configures the start time. This is the time at which the application policy enforcement begins. • end-time – Configures the end time. This is the time at which the application policy enforcement ends. • <HH:MM> – Specify the start and end time in the HH:MM format.

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

no on page 211	Removes this application policy's enforcement period

logging

application-policy on page 195

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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
logging [level|on]
logging on
logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

Parameters

```
logging on
```

logging on	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 on page 211	Resets the logging level to default (notifications). And the `no → logging → on` command disables DPI logging.

mark

application-policy on page 195

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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

```
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]	Uses application category as the match criteria • <APP-CATEGORY-NAME> – 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. • all – The system marks all packets irrespective of the application category.
application <APPLICATION-NAME>	Uses application name as the match criteria • <APPLICATION-NAME> – 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. The WiNG database provides approximately 309 canned applications. In addition to these, the database includes custom-made applications. These are application definitions created using the application on page 183 command.
8021p <0-7>	Marks packets matching the specified criteria with 802.1p priority value • <0-7> – Specify a value from 0 - 7. 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.

dscp <0-63>	Marks packets matching the specified criteria with DSCP ToS code • <0-63> – Specify a value from 0 - 63. 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.
schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this mark rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – 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 > 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time on page 203.

precedence <1-256>	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 *youtube* belonging to app-category *streaming*. The action required is: Allow youtube packets and deny all other applications belonging to app-category streaming.
	The rules can be defined as:
	`#allow application youtube precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application youtube precedence 2`
	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.
	The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

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 on page 211	Removes this mark rule from the application policy

rate-limit

application-policy on page 195

Creates a rate-limit rule and configures the match criteria

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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: *app-category* and *application*.
app-category [<APP-CATEGORY-NAME>|all]	Uses application category as the match criteria • <APP-CATEGORY-NAME> – 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. • all – The system rate-limits all packets irrespective of the application category.

application <APPLICATION-NAME>	Uses application name as the match criteria • <APPLICATION-NAME> – 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.
[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. • egress – Selects the traffic type as outgoing • ingress – Selects the traffic type as outgoing 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: • rate – Configures the rate limit, in Kbps, for both incoming and outgoing packets • <50-1000000> – Specify the rate limit from 50 - 1000000 Kbps.
max-burst-size	The following parameters are common to the 'egress' and 'ingress' keywords: • max-burst-size – Configures the maximum burst size, in Kbytes, for both incoming and outgoing packets • <2-1024> – Specify the maximum burst size from 2 - 1024 Kbytes.

schedule <SCHEDULE-POLICY-NAME>	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. • schedule <SCHEDULE-POLICY-NAME> – 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 > 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time.

precedence <1-256>	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 *youtube* belonging to app-category *streaming*. The action required is: Allow youtube packets and deny all other applications belonging to app-category streaming.
	The rules can be defined as:
	`#allow application youtube precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application youtube precedence 2`
	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.
	The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

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

no on page 211	Removes this rate-limit rule from the application policy

no

application-policy on page 195

Removes or resets this application policy's settings

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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>
```

no <PARAMETERS>	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes this Association ACL Policy

Note
For more information on the association-acl-policy, see Association-ACL Policy on page 1348.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing Auto Provisioning policy

Note

For more information on the auto-provisioning-policy, see Auto-Provisioning Policy on page 1326.

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).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <LIST-NAME> – Provide the AS-PATH-LIST name.
community-list <LIST-NAME>	Creates a community list and enters its configuration mode • <LIST-NAME> – Provide the COMMUNITY-LIST name.
extcommunity-list <LIST-NAME>	Creates an extended community list and enters its configuration mode • <LIST-NAME> – Provide the EXTCOMMUNITY-LIST name.
ip-access-list <LIST-NAME>	Creates a BGP IP access list and enters its configuration mode • <LIST-NAME> – Provide the BGP IP-ACCESS-LIST name.
ip-prefix-list <LIST-NAME>	Creates a BGP IP prefix list and enters its configuration mode • <LIST-NAME> – Provide the BGP IP-PREFIX-LIST name.

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 on page 611	Modifies BGP settings, based on the parameters passed

Note
For more information on the association-acl-policy, see Border Gateway Protocol on page 1867.

ble-data-export-policy

Creates a BLE data export policy and enters its configuration mode. This policy enables forwarding of BLE *(Bluetooth Low Energy)* data to an external, third-party server.

The BLE data export policy provides the external, third-party server's REST URL. After configuring the policy apply it on an RF Domain. Once applied, BLE-enabled, WiNG APs, within the domain, sense BLE iBeacon and Eddystone beacons from other BLE-enabled devices and forward device data to the specified third-party server. This data is forwarded in the JASON format.

Note

The following WiNG access points support BLE data forwarding: AP7632, AP7662

Before enabling BLE data export, ensure that the APs' Bluetooth radio is active and the mode is set to 'le-sensor'. For more information on configuring the Bluetooth settings on the AP's profile/device context, see interface-config-bluetooth-instance on page 1152.

After configuring the policy, in the RF Domain context,

- use the BLE data export policy. For more information, see use (rf-domain-config-mode) on page 488.
- use a sensor policy to define the interval at which data is forwarded. For more information, see use (rf-domain-config-mode) on page 488.

Supported in the following platforms:

- Access Points — AP7612, AP7632, AP7662, AP8432, AP8533

  Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Note

Not supported on AP505 and AP510.

Syntax

```
ble-data-export-policy <POLICY-NAME>
```

Parameters

```
ble-data-export-policy <POLICY-NAME>
```

<POLICY-NAME>	Specify the policy name. If a BLE data export policy with the specified name does not exist, it is created. **Note:** The name should not exceed 32 characters in length.

Examples

```
NOC-NX9500(config)#ble-data-export-policy test
NOC-NX9500(config-ble-data-export-policy-test)#?
Ble Data Export Policy Mode commands:
  no       Negate a command or set its defaults
```

```
  rest     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

NOC-NX9500(config-ble-data-export-policy-test)#
```

Related Commands

no on page 611	Removes an existing BLE data export policy

rest (ble-data-export-commands)

Configures the third-party, BLE-locationing server's URL. This is the external resource to which WiNG APs forward BLE data (UUID, RSSI, etc.) using the REST API. The data is forwarded in the JASON format.

Syntax

```
rest <URL>
```

Parameters

```
rest <URL>
```

rest <URL>	Configures the third-party server's URL • <URL> – Enter the URL. This is the location of the resource to which WiNG APs send real-time RSSI feeds.

Examples

```
ap8432-070235(config-ble-data-export-policy-test)#rest https://test.com/12/
ap8432-070235(config-ble-data-export-policy-test)#show context
ble-data-export-policy test
 rest https://test.com/12/
ap8432-070235(config-ble-data-export-policy-test)#
```

The following example shows the configurations will have to configure the following parameters to enable BLE data forwarding:

1 On the WiNG AP's profile/device context, configure the following Bluetooth parameters:

```
ap8432-070235(config-profile-test-if-bluetooth1)#mode le-sensor
ap8432-070235(config-profile-test-if-bluetooth1)#no shutdown
ap8432-070235(config-profile-test-if-bluetooth1)#show context
 interface bluetooth1
  no shutdown
  mode le-sensor
ap8432-070235(config-profile-test-if-bluetooth1)#
```

This enables the AP as a BLE sensor.

2 On the APs' controller,

a Configure a BLE data export policy, pointing to the external, third-party, REST end-point.

```
NOC-NX9500(config-ble-data-export-policy-test)#rest https://test.com/12/
```

b Configure a sensor policy.

```
NOC-NX9500((config-sensor-policy-test)#rssi-interval-duration 30
```

c Navigate to the BLE-enabled, WiNG AP's RF Domain context and:

- Use the BLE data export policy, configured in step 2a.

```
NOC-NX9500(config-rf-domain-ble)#use ble-data-export-policy test
```

This enables BLE data forwarding to the external, third-party server specified in the policy.

- Use the sensor policy, configured in step 2b.

```
NOC-NX9500(config-rf-domain-ble)#use sensor-policy test
```

When applied, BLE data is forwarded at the interval specified in the sensor policy.

Related Commands

no (ble-data-export-commands) on page 218	Removes the REST endpoint URL configuration
sensor-policy on page 503	Documents the Sensor policy configuration commands

no (ble-data-export-commands)

Removes the BLE data export policy settings

Syntax

```
no rest
```

Parameters

```
no rest
```

no rest	Removes the REST API endpoint's URL (in this case it is the third-party locationing server)

Examples

The following example shows the BLE Data Export policy 'test' settings before the 'no' command is executed:

```
ap8432-070235(config-ble-data-export-policy-test)#show context
ble-data-export-policy test
 rest https://test.com/12/
ap8432-070235(config-ble-data-export-policy-test)#
ap8432-070235(config-ble-data-export-policy-test)#no rest
```

The following example shows the BLE Data Export policy ‘test’ settings after the ‘no’ command was executed:

```
ap8432-070235(config-ble-data-export-policy-test)#show context
ble-data-export-policy test
ap8432-070235(config-ble-data-export-policy-test)#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

Parameters

```
bonjour-gw-discovery-policy <POLICY-NAME>
```

<POLICY-NAME>	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 allow-service 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. Execute the bonjour-gw-forwarding-policy command to enable forwarding of Bonjour service responses across VLANs. To associate a Bonjour GW Discovery policy with a WLAN, in the WLAN configuration mode, execute the following command: `use > bonjour-gw-discovery-policy > <POLICY-NAME>`. For more information, see use (wlan-config-mode) on page 575. To associate a Bonjour GW Discovery policy with a VLAN, in the interface VLAN configuration mode, execute the following command: `use > bonjour-gw-discovery-policy > <POLICY-NAME>`. For more information, see use on page 1057. To associate a Bonjour GW Discovery policy with a user role, in the role-policy - user-role - configuration mode, execute the following command: `use > bonjour-gw-discovery-policy > <POLICY-NAME>`. For more information, see use on page 1631.

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

no on page 611	Removes an existing Bonjour GW Discovery policy

allow-service

Enables discovery of Bonjour devices and the services they provide on Local or Tunneled VLANs

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 <BONJOUR-SERVICE-NAME>	Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered. • <BONJOUR-SERVICE-NAME> – 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. The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner. Use the <WORD> 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).
local	Select to enable the discovery of the selected Bonjour Services on the local VLAN
instance-name contains <WORD>	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. 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). • contains <WORD> – 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 alias on page 172.
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>	Configures the services that can be discovered by the Bonjour gateway. And also configures the VLANs on which the selected services can be discovered. • <BONJOUR-SERVICE-NAME> – 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. The predefined Apple services available are: Afp, AirPlay, AirPort, AirPrint, AirTunes, AppleTimeMachine, Chromecast, Daap, HomeSharing, Printer, and Scanner. Use the <WORD> keyword to define a service not included in the system-provided, predefine list.
tunneled	Select to enable the discovery of the selected Bonjour Services on tunneled VLANs
instance-name contains <WORD>	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). • contains <WORD> – 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 alias on page 172.

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

no on page 611	Removes or modifies this Bonjour Gateway Discovery Policy settings

no

Removes or modifies the Bonjour Gateway Discovery policy settings

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (profile/device-config-mode-commands) on page 1247.

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 on page 611	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
bonjour-gw-query-forwarding-policy <POLICY-NAME>
```

Parameters

```
bonjour-gw-query-forwarding-policy <POLICY-NAME>
```

<POLICY-NAME>	Specify the Bonjour GW Query Forwarding policy name. If the policy does not exist, it is created. 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. To associate a Bonjour GW Query Forwarding policy with a device or profile, in the profile/device configuration mode, execute the `use > bonjour-gw-query-forwarding-policy > <POLICY-NAME>` command. For more information, see use (profile/device-config-mode-commands) on page 1247.

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

no on page 611	Removes an existing Bonjour GW Query Forwarding policy

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 is a browser-based authentication mechanism that forces unauthenticated users to a web page. Captive portals capture and re-direct a wireless user's web-browser session to a captive portal login page where the user must enter valid credentials to access the wireless network. Once logged into the captive portal, additional *Acknowledgment*, *Agreement*, *Welcome*, *No Service* and *Fail* customized pages enhance screen flow and user experience.

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.

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:
  access-time                 Allowed access time for the client. Used when
                              there is no session time in radius response
  access-type                 Access type of this captive portal
  accounting                  Configure how accounting records are created for
                              this captive portal policy
  bypass                      Bypass captive portal
  connection-mode             Connection mode for this captive portal
  custom-auth                 Custom user information
  data-limit                  Enforce data limit for clients
  frictionless-onboarding     Register the client MAC address at ExtremeGuest
                              on redirection
  inactivity-timeout          Inactivity timeout in seconds. If a frame is not
                              received from client for this amount of time,
                              then current session will be removed
  ipv6                        Internet Protocol version 6 (IPv6)
  localization                Configure the FQDN address to get the
                              localization parameters for the client
  logout-fqdn                 Configure the FQDN address to logout the session
                              from client
  no                          Negate a command or set its defaults
  oauth                       OAuth 2.0 authentication configuration
  php-helper                  Configure the captive portal to use a server for
                              help with php
  post-authentication-vlan    Configure post authentication vlan for captive
                              portal users
  radius-vlan-assignment      Enable radius vlan assignment for captive portal
                              users
  redirection                 Configure connection redirection parameters
  report-loyalty-application  Report customer loyalty application presence in
                              clients
  server                      Configure captive portal server parameters
```

```
  simultaneous-users          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

no on page 611	Removes an existing captive portal

captive-portal-mode-commands

The following table summarizes captive portal configuration mode commands:

Table 7: Captive-Portal-Mode Commands

Command	Description
access-time on page 229	Defines a client's access time. It is used when no session time is defined in the RADIUS response.
access-type on page 229	Configures a captive portal's access type
accounting on page 230	Enables a captive portal's accounting records
bypass on page 231	Enables bypassing of captive portal detection requests
connection-mode on page 232	Configures a captive portal's connection mode
custom-auth on page 232	Configures custom user information
data-limit on page 233	Enforces data limit on captive portal clients
frictionless-onboarding on page 234	Enables wireless clients, associated with guest WLANs, to self-register with the ExtremeGuest server.
inactivity-timeout on page 237	Defines an inactivity timeout in seconds
ipv6 on page 237	Configures the IPv6 address of the internal captive portal server
localization on page 238	Configures an FQDN address string that enables the client to receive localization parameters. This command also allows the configuration of a response message.

Table 7: Captive-Portal-Mode Commands (continued)

Command	Description
logout-fqdn on page 240	Clears the logout FQDN address
no on page 261	Reverts the selected captive portal's settings or resets settings to default
oauth on page 240	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.
php-helper on page 242	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.
post-authentication-vlan on page 243	Assigns a post authentication RADIUS VLAN for this captive portal's users
radius-vlan-assignment on page 244	Assigns a RADIUS VLAN for this captive portal
redirection on page 245	Enables redirection of client connections to specified destination ports
report-royalty-application on page 245	Enables detection of captive portal client's loyalty application presence and stores this information in the captive portal's user database
server on page 246	Configures the captive portal server settings
simultaneous-users on page 248	Specifies a username used by a MAC address pool
terms-agreement on page 249	Enforces the user to agree to terms and conditions (included in login page) for captive portal access
use (captive-portal-config-mode) on page 250	Associates a AAA policy and a DNS whitelist with a captive portal
webpage on page 251	Configures captive portal Web page settings
webpage-auto-upload on page 259	Enables automatic upload of advanced Web pages on a captive portal
webpage-location on page 260	Specifies the location of Web pages used for captive portal authentication
welcome-back on page 260	Enables the provision of direct Internet access to once-registered, captive-portal guest users on subsequent log-ins
configuring-device-registration-with-dynamic-vlan-assignment on page 263	Provides the configuration details required to enable device registration with dynamic VLAN assignment in a multi-vendor environment.
configuring WeChat Wi-Fi hotspot support in WiNG captive portal on page 265	Provides configuration detals required to enable WeChat Wi-Fi hotspot support in WiNG captive portal.
configuring ExtremeGuest captive portal on page 267	Provides the basic configurations required to deploy an *ExtremeGuest* setup

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
access-time <10-10080>
```

Parameters

```
access-time <10-10080>
```

<30-10080>	Defines the access time allowed for a wireless client from 10 - 10080 minutes. The default is 1440 minutes.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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. If enabled, use the **webpage > internal > registration > field** 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • host <IP/HOSTNAME> – Specifies the destination where accounting messages are sent. Specify the destination's IP address or hostname.
port <1-65535>	Optional. Specifies the syslog server's listener port • <1-65535> – Specify the UDP port from 1- 65535. The default is 514.
proxy-mode [none| through-controller| through-rf-domain-manager]	Optional. Specifies the mode of proxying the syslog server • none – Accounting messages are sent directly to the syslog server • through-controller – Accounting messages are sent through the controller configuring the device • through-rf-domain-manager – Accounting messages are sent through the local RF Domain manager

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 Note: 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
custom-auth info <LINE>
```

Parameters

```
custom-auth info <LINE>
```

info <LINE>	Configures information used for RADIUS lookup when *custom-auth RADIUS* access type is configured • <LINE> – Guest data needs to be provided. Specify the *name*, *e-mail address*, and *telephone number* of the user.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

Parameters

```
data-limit <1-102400> {action [log-and-disconnect|log-only]}
```

data-limit <1-102400>	Sets a captive portal client's data transfer limit in megabytes. This limit is applicable for both upstream and downstream data transfer. • <1-102400> – Specify a value from 1 - 102400 MB.
action [log-and-disconnect| log-only]	Optional. Specifies the action taken when a client exceeds the configured data limit. The options are: • 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. • 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.

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

no	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 infomration on enabling frictionless-onboarding, see Examples on page 234.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 URl.

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

no on page 261	Disables frictionless-onboarding of guest users to the ExtremeGuest server

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
inactivity-timeout <60-86400>
```

Parameters

```
inactivity-timeout <60-86400>
```

<60-86400>	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. • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 10 minutes or 600 seconds.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ipv6 server host <IPv6>
```

Parameters

```
ipv6 server host <IPv6>
```

ipv6 server host <IPv6>	Configures the IPv6 address of the internal captive portal server • <IPv6> – Specify the captive portal server's global IPv6 address.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <WORD> – Specify the FQDN address string. For example, local.guestaccess.com
response <WORD>	Configures the response message directed back to the client for localization HTTP requests. • <WORD> – Specify the response message (should not exceed 512 characters in length). The following built-in query tags can be included in the response message: 'WING_TAG_CLIENT_IP' -Captive portal client IPv4 address 'WING_TAG_CLIENT_MAC' - Captive portal client MAC address 'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid 'WING_TAG_AP_MAC' - Captive portal client AP MAC address 'WING_TAG_AP_NAME' - Captive portal client AP Name 'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain 'WING_TAG_USERNAME' - Captive portal authentication username 'WING_TAG_USERTYPE' - Captive portal usertype (new/return/refresh) Example:- <local><site>WING_TAG_RF_DOMAIN</site><ap>WING_TAG_AP_NAME</ap></local

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Configures the client-ids retrieved from the Google and Facebook API manager portals during registration • facebook – Configures the Facebook API client-id (is a 15 digit entity) • google – Configures the Google API client-id (is a 12 digit number) • <WORD> – Provide the Facebook/Google client-id. 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.

Example (User Exec Mode)

```
nx7500-6DCD39(config-captive-portal-test2)#OAuth
nx7500-6DCD39(config-captive-portal-test2)#OAuth client-id Google
xxxxxxxxxxxx.apps.googleusercontent.com Facebook yyyyyyyyyyyyyyy
nx7500-6DCD39(config-captive-portal-test2)#show context
captive-portal test2
 server host guest.social.com
  oauth
  oauth client-id Google xxxxxxxxxxxx.apps.googleusercontent.com Facebook yyyyyyyyyyyyyyy

nx7500-6DCD39(config-captive-portal-test)#
```

In the above example,

- xxxxxxxxxxxx - Is the 12 digit numeric part of your Google client-id.
- yyyyyyyyyyyyyyy - 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.
- 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 (NX9500/NX9600/VX9000) enabled as the EGuest server.

For more information on enabling the EGuest server, see eguest-server (VX9000 only) on page 987.

For more information on configuring an EGuest captive portal, see configuring ExtremeGuest captive portal on page 267.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <IP/HOSTNAME> – Specify the adopting controller’s IP address or host name.
hosting-vlan-interface <0-4096>	Optional. Configures the VLAN on which the php-helper is reachable • <0-4096> – Specify the VLAN hosting the php-helper from 0 - 4096.

```
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 • <IP/HOSTNAME> – Specify the RF Domain manager's IP address or host name.

Examples

To enable php-helper configure the following parameters in the captive-portal context:

```
ap505-13403B(config-captive-portal-php-helper)#oauth
ap505-13403B(config-captive-portal-php-helper)#php-helper controller nx9500-6C8809
ap505-13403B(config-captive-portal-php-helper)#server mode self
ap505-13403B(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.

```
ap505-13403B(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--
ap505-13403B(config-captive-portal-php-helper)#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]
```

Parameters

```
post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]
```

post-authentication-vlan [<1-4096>|<VLAN-ALIAS>]	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. • <1-4096> – Specify the VLAN's number from 1 - 4096. • <VLAN-ALIAS> – Specify the VLAN alias (should be existing and configured). VLAN alias names begin with a '$'.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
redirection ports <LIST-OF-PORTS>
```

Parameters

```
redirection ports <LIST-OF-PORTS>
```

ports <LIST-OF-PORTS>	Configures destination ports considered for redirecting client connection 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
report-loyalty-application {custom-app <APPLICATION-NAME>}
```

Parameters

```
report-loyalty-application {custom-app <APPLICATION-NAME>}
```

report-loyalty-application {custom-app <APPLICATION-NAME>}	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. • custom-app <APPLICATION-NAME> – Optional. Uses a custom application definition as match criteria. • <APPLICATION-NAME> – 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 application on page 183. If no custom application definition is specified, the system uses localization to detect application presence.

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 on page 261	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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/HOSTNAME>	Configures the internal captive portal server (wireless controller, access point, service platform) • <IP/HOSTNAME> – Specify the IPv4/IPv6 address or hostname of the captive portal server. For centralized-controller mode, the server host should be a virtual hostname and not an IP address. 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 oauth and php-helper.

```
server mode [centralized|centralized-controller {hosting-vlan-interface <0-4096>}|self]
```

mode	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 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.
centralized	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. Ensure the IPv4 address or hostname of the wireless controller performing the capture and redirection is defined in the captive portal policy. And also, that the wireless controller is reachable via MINT.

centralized-controller {hosting-vlan-interface <0-4096>}	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. 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. • 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. • <0-4096> – Specify the VLAN number (0 implies the controller is available on the client's VLAN).
self	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. 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.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
simultaneous-users <1-8192>
```

Parameters

```
simultaneous-users <1-8192>
```

simultaneous-users <1-8192>	Specifies the number of MAC addresses that can simultaneously access the captive portal • <1-8192> – Select a number from 1 - 8192.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no	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.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <AAA-POLICY-NAME> – Specify the AAA policy name. For more information on AAA policies, see AAA Policy on page 1303.
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. • <DNS-WHITELIST-NAME> – Specify the DNS whitelist name. 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. For more information on DNS whitelists, see dns-whitelist.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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	Indicates the page is displayed for “Terms & Conditions” The agreement page provides conditions that must be agreed to before captive portal access is permitted.
fail	Indicates the page is displayed for login failure 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.
login {post}	Indicates the page is displayed for getting user credentials. This page is displayed by default. • post – Optional. Redirects users to post externally when they during authentication 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.
no-service	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: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring. • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring. • AP to controller connectivity monitoring. For more information on enabling these critical resource monitoring, see service.
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. 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 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. Supported Query Tags are: 'WING_TAG_CLIENT_IP' - Captive portal client IPv4 address 'WING_TAG_CLIENT_MAC' - Captive portal client MAC address 'WING_TAG_WLAN_SSID ' - Captive portal client WLAN ssid 'WING_TAG_AP_MAC' - Captive portal client AP MAC address 'WING_TAG_AP_NAME' - Captive portal client AP Name 'WING_TAG_RF_DOMAIN' - Captive portal client RF Domain 'WING_TAG_CP_SERVER' - Captive portal server address 'WING_TAG_USERNAME' - Captive portal authentication username Example: http://cportal.com/policy/login.html?client_ip=WING_TAG_CLIENT_IP&ap_mc=WING_TAG_AP_MAC. Use '&' or '?' character to separate field-value pair. 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: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring. • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring. • AP to controller connectivity monitoring. For more information on enabling these critical resource monitoring, see service.
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 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: • <CONTENT> – 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.

```
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: • The RADIUS server (on-board or external) is not reachable and the user cannot be authenticated • The external captive portal server is not reachable • The connectivity between the adopted AP and controller is lost • The external DHCP server is not reachable To provide this service, enable the following: • External captive portal server monitoring. • AAA server monitoring. This enables detection of RADIUS server failure. • External DHCP server monitoring. • AP to controller connectivity monitoring. For more information on enabling these critical resource monitoring, see service.
registration	Indicates the page displayed is the registration page to which users are redirected in order to register in the captive portal’s database 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: • main-logo – Indicates the main logo displayed in the header of each Web page • use-as-banner – Uses the image, specified here, as the Web page banner, in place of the logo and organization name

small-logo	The following keyword is common to all of the above internal Web page options: • small-logo – Indicates the logo image displayed in the footer portion of each Web page, and constitutes the organization's signature
<URL>	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. • <URL> – Specify the location and name of the main-logo and the small-logo image files.

```
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	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.) 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. If the registration Web page is not customized, the built-in, default registration page is displayed to the client.

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

	• optout – Creates an input field that enables clients to opt out from registering
	  • checkbox – Configures the optout field as a check box
	• street – Creates the postal address: street name/number input field (enabled by default and included in the built-in registration page)
	  • text – Configures the street field as only alpha-numeric and special characters input field
	• 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)
	  • checkbox – Configures the via-email field as a check box
	• 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)
	  • checkbox – Configures the via-sms field as a check box
	• zip – Creates the postal address: zip input field (enabled by default and included in the built-in registration page)
	  • number – Configures the zip field as only-numeric characters input field
	  • text – Configures the zip field as only alpha-numeric and special characters input field

type [checkbox|date| dropdown-menu|e-address|number| radio-button|text]	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. • checkbox – Configures the field as a check box • date – Configures the field as only date-format input field • dropdown-menu – Configures the field as a drop-down menu • e-address – Configures the field as an e-mail address input field • number – Configures the field as only-numeric characters input field • radio-button – Configures the field as a radio button • text – Configures the field as only alpha-numeric and special characters input field 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.
enable {label <LINE>| mandatory| title <LINE>| placeholder <LINE>}	Enables the field. When enabled, the field is displayed on the registration page. After enabling the field, optionally configure the following parameters: • label <LINE> – Optional. Configures the field's label • mandatory – Optional. Makes the field mandatory • title – Optional. Configures the comma-separated list of items to include in the drop-down menu. • placeholder <LINE> – Optional. Configures a string, not exceeding 300 characters, that is displayed within the field. If not configured, the field remains blank.

```
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. Use the **webpage > external > welcome > <URL>** 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-ca-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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no	Disables automatic upload of advanced Web pages on a captive portal
webpage	Configures Web pages displayed when interacting with a captive portal
webpage-location	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
webpage-location [advanced|external|internal]
```

Parameters

```
webpage-location [advanced|external|internal]
```

advanced	Uses Web pages for login, welcome, failure, and terms created and stored on the controller. Select advanced 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. If selecting advanced, enable the webpage-auto-upload option to automatically launch the advanced pages to requesting clients upon association. For more information, see webpage-auto-upload.
external	Uses Web pages for login, welcome, failure, and terms located on an external server. Provide the URL for each of these pages.
internal	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

no	Resets or disables captive portal Web page settings
webpage	Configures a captive portal's Web page (acknowledgment, agreement, login, welcome, fail, no-service, and terms) settings
webpage-auto-upload	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, AP7632, AP7662, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 7510, NX 95XX, NX 96XX, VX

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 • pass-through – Provides user direct Internet access, from the Welcome-back page, without any user action

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

The no command reverts the selected captive portal's settings or resets settings to default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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-ge1)#switchport mode trunk
nx9500-6C8809(config-profile-SITE-10-if-ge1)#switchport trunk native vlan 90
nx9500-6C8809(config-profile-SITE-10-if-ge1)#switchport trunk allowed vlan
1,90,1000-1002
nx9500-6C8809(config-profile-SITE-10-if-ge1)#no switchport trunk native tagged
```

8 Use the access point profile in the access point's device context.

Related Commands

radius-server-policy on page 1566	Documents RADIUS server policy configuration commands
radius-group on page 1558	Documents RADIUS group policy configuration commands
radius-user-pool-policy on page 1583	Documents RADIUS user policy configuration commands
AAA Policy on page 1303	Documents AAA policy configuration commands
captive-portal on page 225	Documents captive-portal configuration commands

wlan on page 518	Documents WLAN configuration commands
Profiles on page 848	Documents profile configuration commands
guest-registration on page 732 (show commands)	Documents `show > guest-registration` 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 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 *independent software vendor* (ISV), 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 parameters in the captive portal created in step 3:

```
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:

AAA Policy on page 1303	Documents AAA policy configuration mode commands
dns-whitelist on page 310	Documents DNS whitelist configuration mode commands
captive-portal on page 225	Documents captive portal configuration mode commands
wlan on page 518	Documents WLAN configuration mode commands

configuring ExtremeGuest captive portal

This section documents the basic configurations required to deploy an *ExtremeGuest* (EGuest) 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 VX9000 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-EguestWLAN)#
```

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.

```
Eguest-AP(config-device-74-67-F7-5C-64-4A)#use captive-portal EguestCP
```

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:

AAA Policy on page 1303	Documents AAA policy configuration mode commands
dns-whitelist on page 310	Documents DNS whitelist configuration mode commands
captive-portal on page 225	Documents captive portal configuration mode commands
wlan on page 518	Documents WLAN configuration mode commands
eguest-server (VX9000 only) on page 987	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.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
clear event-history
```

Parameters

```
clear event-history
```

event-history	Clears the event history file

Examples

```
nx9500-6C8809(config)#show event-history
EVENT HISTORY REPORT
Generated on '2019-02-21 14:21:03 UTC' by 'admin'

2019-02-21 14:20:50     nx9500-6C8809  SYSTEM     LOGIN                Successfully
logged in user 'admin' with privilege 'superuser' from 'ssh'
2019-02-21 14:12:46     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 14:02:42     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 13:52:38     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 13:42:33     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
```

```
2019-02-21 13:32:29     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 13:22:25     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 13:12:21     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 13:02:18     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
2019-02-21 12:52:10     nx9500-6C8809  DIAG       PWRSPLY_FAIL         Power supply
redundancy failure
--More--
nx9500-6C8809(config)#
nx9500-6C8809(config)#clear event-history
nx9500-6C8809(config)#show event-history
EVENT HISTORY REPORT
Generated on '2019-02-21 14:21:40 UTC' by 'admin'

nx9500-6C8809(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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-identity <CLIENT-IDENTITY-NAME>
```

Parameters

```
client-identity <CLIENT-IDENTITY-NAME>
```

client-identity <CLIENT-IDENTITY-NAME>	Creates a new client identity policy and enters its configuration mode • <CLIENT-IDENTITY-NAME> – Specify a client identity policy name. If the client identity policy does not exist, it is created.

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 on page 546.
- 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 identity 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
nx9500-6C8809(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

nx9500-6C8809(config-client-identity-test)#
```

Note

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

no on page 611	Removes an existing client identity definition
client-identity-group on page 277	Configures a new client identity group

client-identity-mode-commands

The following table summarizes the client-identity configuration mode commands:

Table 8: Client-Identity-Mode Commands

Command	Description
dhcp on page 274	Configures the DHCP option match criteria for device fingerprinting
dhcp-match-message-type on page 275	Configures the DHCP message type for device fingerprinting
no (client-identity-config-mode) on page 276	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 *Operating System* (OS). 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Adds a DHCP option match criteria signature • <1-16> – Specify an index for this DHCP match criteria from 1 - 16. **Note:** A maximum of 16 match criteria can be configured.
message-type [discover|request]	Specifies the message type to which this DHCP match criteria is applicable • 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. • 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. **Note:** It is recommended to configure client-identity with request messages, because clients rarely send discover messages. **Note:** If the message type is not specified, the fingerprint is checked with all message types (DHCP request and DHCP discover).
option <1-254>	The following keywords are common to the 'discover' and 'request' message types: • option – Configures a DHCP option value, which is used as the match criteria • <1-254> – Configures a code for this DHCP option from 1 - 254 (except option 53)
option-codes	The following keyword is common to the 'discover' and 'request' message types: • option-codes – Matches criteria based on the DHCP option codes contained in the client's discover/request messages 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.

contains	The following keyword is common to the 'discover' and 'request' message types: • contains – Specifies that the DHCP options received in the client's discover/request messages contains the configured option code string
exact	The following keyword is common to the discover and request message types: • exact – Specifies that the DHCP options received in the client's discover/request messages is an exact match with the configured option code string
starts-with	The following keyword is common to the 'discover' and 'request' message types: • starts-with – Specifies that the DHCP options received in the client's discover/request messages starts with the configured option code string
ascii <WORD>	The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters: • ascii – Configures the DHCP option in the ASCII format • <WORD> – Specify the DHCP option ASCII value to match.
hexstring <WORD>	The following keywords are common to the 'contains', 'exact', and 'starts-with' parameters: • hexstring – Configures the DHCP option in the hexa-decimal format • <WORD> – Specify the DHCP option hexstring value to match.

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

```
nx9500-6C8809(config-client-identity-test)#dhcp 1 message-type request option
60 exact ascii MSFT\5.0
nx9500-6C8809(config-client-identity-test)#dhcp 2 message-type discover option
 2 exact hexstring 012456c22c44
nx9500-6C8809(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
nx9500-6C8809(config-client-identity-test)#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]	Specifies the DHCP message type to consider for matching • all – Matches all message types: discover and request. Indicates that the fingerprint is checked with both the DHCP request and the DHCP discover message. • any – Matches any message type: discover or request. Indicates that the fingerprint is checked with either the DHCP request or the DHCP discover message. • 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. • 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.

Examples

```
nx9500-6C8809(config-client-identity-test)#dhcp-match-message-type all
nx9500-6C8809(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
nx9500-6C8809(config-client-identity-test)#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [dhcp <1-16>|dhcp-match-message-type]
```

Parameters

```
no [dhcp <1-16>|dhcp-match-message-type]
```

dhcp <1-16>	Removes the DHCP option match criteria rule identified by the <1-16> keyword • <1-16> – Specify the DHCP option match criteria rule index
dhcp-match-message-type	Removes the DHCP message type to match

Examples

The following example shows the client identity 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(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
nx9500-6C8809(config-client-identity-test)#
```

The following example shows the client identity 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-client-identity-test)#no dhcp 2
nx9500-6C8809(config-client-identity-test)#no dhcp-match-message-type
nx9500-6C8809(config-client-identity-test)#show context
client-identity test
 dhcp 1 message-type request option 60 exact ascii MSFT5.0
nx9500-6C8809(config-client-identity-test)#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

Parameters

```
client-identity-group <CLIENT-IDENTITY-GROUP-NAME>
```

client-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Creates a new client identity group and enters its configuration mode • <CLIENT-IDENTITY-GROUP-NAME> – Specify a client identity group name. If the group does not exist, it is created.

Examples

```
nx9500-6C8809(config)#client-identity-group test
nx9500-6C8809(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

nx9500-6C8809(config-client-identity-group-test)#
```

Related Commands

no on page 611	Removes an existing client identity group

client-identity-group-mode-commands

The following table summarizes the client identity group configuration mode commands:

Table 9: Client-Identity-Group-Mode Commands

Command	Description
client-identity on page 278	Associates an existing and configured client identity (device fingerprinting definition) with this client identity group
load on page 280	Loads default (system-provided) client identity fingerprints
no (client-identity-group-config-mode) on page 281	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

Parameters

```
client-identity <CLIENT-IDENTITY-NAME> precedence <1-10000>
```

client-identity <CLIENT-IDENTITY-NAME>	Associates a client identity with this group • <CLIENT-IDENTITY-NAME> – Specify a client identity name (should be existing and configured)
precedence <1-10000>	Determines the order in which client identity is used. • <1-10000> – Specify this client identity precedence 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 priority over a client identity having precedence 20.

Examples

The following example shows two client identities created and configured:

```
nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 7.1.0.0-010D
!
!
version 2.6
!
!
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--
nx9500-6C8809(config)#
```

The following example associates client identity ‘test’ with the client identity group ‘test’:

```
nx9500-6C8809(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:

```
nx9500-6C8809(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
nx9500-6C8809(config-client-identity-group-test)#
```

Related Commands

no	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 if applied to a device (either directly or through the profile).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

Note

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
nx9500-6C8809((config-client-identity-group-test)#show context
client-identity-group test
 client-identity test precedence 1
<exsw5>(config-client-identity-group-test)#

nx9500-6C8809((config-client-identity-group-test)#no client-identity test
```

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

TLO <EXISTING-OBJECT-NAME> <NEW-OBJECT-NAME>	Creates a new TLO by cloning an existing top-level object. The new object has the same configuration as the cloned object. • <EXISTING-OBJECT-NAME> – Specify the existing object's (to be cloned) name • <NEW-OBJECT-NAME> – Provide the new object's name. Note: Enter `clone` and press **Tab** to list objects available for cloning.

```
clone device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>
```

device <EXISTING-DEVICE-MAC/NAME> <NEW-DEVICE-MAC>	Configures a new device based on an existing device configuration • <EXISTING-DEVICE-MAC/NAME> – Specify the existing device's name or MAC address (the device to be cloned) • <NEW-DEVICE-MAC> – Provide the new device's MAC address. Note: Enter `clone > device` and press **Tab** to list devices available for cloning.

Examples

```
nx9500-6C874D(config)#clone rf_domain TechPubs Cloned_TechPubs2
nx9500-6C874D(config)#show context
!
! Configuration of NX9500 version 7.1.0.0-010D
!
!
version 2.6
!
.....................................................................................
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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

Parameters

```
crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>	Specify the crypto CMP policy name. If the policy does not exist, it is created.

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 on page 611	Resets values or disables commands

Note

For more information on the crypto CMP policy, see Crypto-CMP Policy on page 1846.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-64> – Sets the hostname column width from 1 - 64 characters
cdp-lldp-info-column-width <1-64>	Configures the column width in the **show > cdp/lldp > [neighbor|report]** command output • <1-64> – Sets the column width from 1 - 64 characters

```
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 **show > wireless > client** command output 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 • <1-64> – Sets the ap-name column width from 1 - 64 characters
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 client-identity. • <1-32> – Sets the client-identity column width from 1 - 32 characters
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 • <1-64> – Sets the hostname column width from 1 - 64 characters
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 • <1-64> – Sets the location column width from 1 - 64 characters
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 • <3-67 – Sets the radio-alias column width from 3 - 67 characters
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 • <1-32> – Sets the role column width from 1 - 32 characters
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 • <1-64> – Specify the username column width from 1 - 64 characters.
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 **show > wireless > client** stats command output 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 • <1-64> – Sets the hostname column width from 1 - 64 characters
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 **show > wireless > client** stats RF command output 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 • <1-64> – Sets the hostname column width from 1 - 64 characters
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 Note: 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 *signal-to-noise* (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 **show > wireless > meshpoint > accelerated multicast** 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. 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 **show > wireless > meshpoint** command output 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 • <1-64> – Sets the hostname column width from 1 - 64 characters
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 • <1-64> – Sets the mesh-name column width from 1 - 64 characters
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) • <1-64> – Sets the next-hop-hostname column width from 1 - 64 characters
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 • <1-64> – Sets the root-hostname column width from 1 - 64 characters
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 **show > wireless > meshpoint > neighbor > stats** command output 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 • <1-64> – Sets the ap-name column width from 1 - 64 characters
neighbor-hostname <1-64>	Includes the neighbor-hostname column, which displays the reported neighbor's hostname • <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters
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 **show > wireless > meshpoint > neighbor > statistics RF** command output 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 • <1-64> – Sets the ap-name column width from 1 - 64 characters
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 • <1-64> – Sets the neighbor-hostname column width from 1 - 64 characters
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 **show > wireless > mint > client** 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 **show > wireless > mint > client > statistics** 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 **show > wireless > mint > client > statistics > rf** 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 **show > wireless > mint > portal** 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 **show > wireless > mint > portal > statistics > rf** 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 • <1-64> – Sets the ap-name column width from 1 - 64 characters
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 • <1-64> – Sets the location column width from 1 - 64 characters
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) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
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) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
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 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) • <3-67> – Sets the radio-alias column width from 3 - 67 characters
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

no on page 611	Restores custom CLI settings to default

database-client-policy global-config

Creates a database-client-policy and enters its configuration mode. The database-client-policy is only needed in deployments implementing captive-portal registration and database authentication with an onboard database. If enforcing database authentication, configure the user-name and password required to access the database on the database-client-policy.

Note
For more information on enabling database authentication, see Example: Enabling Database Authentication on page 68.

Supported in the following platforms:

- Service Platforms — NX9500, NX9600, VX9000

Syntax

```
database-client-policy <DATABASE-CLIENT-POLICY-NAME>
```

Parameters

```
database-client-policy <DATABASE-CLIENT-POLICY-NAME>
```

database-client-policy <DATABASE-CLIENT-POLICY-NAME>	Specify the database-client-policy name. If the policy does not exist, it is created. Once created and configured, apply this policy on the device hosting the database.

Examples

```
vx9000-34B78B(config)#database-client-policy DBClientPolicy
vx9000-34B78B(config-database-client-policy-DBClientPolicy)#?
Database Client Policy Mode commands:
  authentication   Database authentication
  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)#
```

Related Commands

no on page 611	Removes an existing database-client-policy
database-policy global config on page 299	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.
use (profile/device-config-mode-commands) on page 1247	Uses a database-client-policy in the VX9000's device or profile context
database on page 66	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 zerzoise the keyfile.

database-client-policy-commands

The following table summarizes database-client-policy configuration mode commands:

Table 10: Database Client Policy Config Commands

Command	Description
authentication on page 297	Configures the captive-portal/NSight database users
no (database-client-policy-config-mode) on page 298	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 — NX9500, NX9600, VX9000

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 623 (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 299. **Note:** For more information on enabling database authentication, see Example: Enabling Database Authentication on page 68.

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

no	Removes an existing database username and password

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 Example: Enabling Database Authentication on page 68.

Supported in the following platforms:

- Service Platforms — NX9500, NX9600, VX9000

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 with the specified name does not exist, it is created.

Examples

```
nx9500-6C8809(config)#database-policy test
nx9500-6C8809(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
nx9500-6C8809(config-database-policy-test)#
```

Related Commands

no on page 611	Removes an existing database-policy
database-client-policy global-config on page 296	Documents database-client policy configuration commands. The database-client-policy configures the IP address or hostname of the database host, and is used on the EGuest server's device context.
use (profile/device-config-mode-commands) on page 1247	Uses a database-client-policy in the VX9000's device or profile context
database on page 66	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 zerzoise the keyfile.

database-policy-config-commands

The following table summarizes database-policy configuration mode commands:

Table 11: Database Policy Config Commands

Command	Description
authentication on page 300	Enables database authentication and configures the username and password required to access the database
replica-set on page 301	Adds a member to a database replica set
shutdown on page 303	Shuts down the database server
no (database-policy-config-mode) on page 303	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 — NX9500, NX9600, VX9000

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>	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 service (common commands). • username <USER-NAME> – Configures the database username • password <PASSWORD> – Configures the password for the username specified above 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 database-client-policy global-config on page 296. For more information on enabling database authentication, see Example: Enabling Database Authentication on page 68.

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>}
```

replica-set member [<IP>|<FQDN>] {arbiter|priority <0-255>}	Adds a member to the database replica set. To identify the member, use one of the following options: • <IP> – Specify the member's IP address. • <FQDN> – Specify the member's FQDN. After specifying the IP address or FQDN, specify the following: • arbiter – Optional. Select to configure the member as the arbiter. • priority <0-255> – Optional. Configures the priority of a non-arbiter member of the replica set • <0-255> – 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. 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.

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

no	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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
device {containing|filter}
device {containing <STRING>} {filter type [ap505|ap510|ex3524|ex3548|rfs4000|nx5500|
nx75xx|nx9000|nx9600|t5|vx9000]}
device {filter type [ap505|ap510|ex3524|ex3548|rfs4000|nx5500|nx75xx|nx9000|nx9600|
t5|vx9000]}
```

Parameters

```
device {containing <STRING>} {filter type [ap505|ap510|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. • <STRING> – Specify the string to search for in the device's hostname.
filter type <DEVICE-TYPE>	Optional. Filters out a specific device type. After specifying the hostname string, select the device type. The options are: AP510, AP505, EX3424, EX3548, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000, and T5.

```
device  {filter type [ap505|ap510|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: AP510, AP505, EX3424, EX3548, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000, and T5..

Examples

```
ap505-13403B(config)#device filter type ap5
ap510  ap505
ap505-13403B(config)#device filter type ap505 ?
  <cr>

ap505-13403B(config)#device filter type ap505
ap505-13403B(config-device-{'type': 'ap505'})#
```

Related Commands

no on page 611	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing device categorization list

device-categorization-mode-commands

The following table summarizes device categorization configuration mode commands:

Table 12: Device-Categorization Config Mode Commands

Command	Description
mark-device on page 306	Adds a device to the device categorization list
no (device-categorization-config-mode) on page 307	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}	Marks a specified AP as sanctioned or neighboring based on its MAC address or the SSID it is beaconing • mac <MAC> – Optional. Specify the AP's MAC address • ssid <SSID> – Optional. Specify the SSID the AP is beaconing. After specifying the SSID, you can optionally specify MAC address of the radio. All APs are marked if no specific MAC address or SSID is provided.

```
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 • mac <MAC> – Optional. Specify the wireless client's MAC address.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing DHCP server policy

Note
For more information on DHCPv4 policy, see DHCP-Server Policy on page 1425 .

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing DHCPv6 server policy

Note
For more information on DHCPv6 policy, see DHCP-Server Policy on page 1425.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dns-whitelist <DNS-WHITELIST-NAME>
```

Parameters

```
dns-whitelist <DNS-WHITELIST-NAME>
```

<DNS-WHITELIST-NAME>	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

no on page 611	Removes an existing DNS Whitelist

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

Parameters

```
permit <IPv4/IPv6/HOSTNAME> {suffix}
```

<IPv4/IPv6/ HOSTNAME>	Adds a device to the DNS whitelist • <IPv4/IPv6/HOSTNAME> – Provide a hostname or numerical IPv4 or IPv6 address for each destination IP address or host included in the whitelist. Note: A maximum of 256 entries can be made.
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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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) • <IPv4/IPv6/HOSTNAME> – Specify the device's IPv4/IPv6 address or hostname.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
end
```

Parameters

```
None
```

Examples

```
rfs4000-229D58(config)#end
rfs4000-229D58#
```

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 SEP *(Small Form-factor Pluggable)* transceiver slots for fiber connectivity. The EX3500 series switch can adopt to a 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 rules, see ex3500 (mac-acl-config-commands) on page 1391 and #unique_321.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

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 • <TIME-RANGE-NAME> – Enter a name for this time range. If the time range does not exist, it is created.

Examples

```
nx9500-6C8809(config)#ex3500 time-range EX3500_TimeRange_02
nx9500-6C8809(config-ex3500-time-range-EX3500_TimeRange_02)#?
nx9500-6C8809 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

no on page 611	Removes this EX3500 time range list

ex3500-time-range-config-commands

Table 13: EX3500 Time Range Config Commands

Command	Description
absolute on page 314	Configures an absolute time range rule for this EX3500 time range list
periodic on page 315	Configures a periodic time range rule for this EX3500 time range list
no (ex3500-time-range-config-mode) on page 317	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 7510, NX 95XX, NX 96XX

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> <MONTH> <2013-2037>	Configures the start day and time settings • <0-23> – Specify the start time from 0 - 23 hours. • <0-59> – Specify the start time from 0 - 59 minutes. For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day. • <1-31> – Specify the day of month from 1 - 31 when the time range starts. • <MONTH> – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September. <2013-2037> – Specify the year from 2013 - 2037.
end <0-23> <0-59> <1-31> <MONTH> <2013-2037>	Optional. Configures the end day and time settings • <0-23> – Specify the end time from 0 - 23 hours. • <0-59> – Specify the end time from 0 - 59 minutes. • <1-31> – Specify the day of month from 1 - 31 when the time range ends. • <MONTH> – Specify the month. The options are: April, August, December, February, January, July, June, March, May, November, October, September. <2013-2037> – Specify the year from 2013 - 2037.

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 (ex3500-time-range-config-mode) on page 317	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 7500, NX 95XX, NX 96XX

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>
```

periodic [daily|friday|monday| saturday|sunday| thursday| tuesday| wednesday| weekdays| weekend]	Configures this periodic time range's start day. The options are: • daily • Friday • Monday • Saturday • Sunday • Thursday • Tuesday • Wednesday • weekdays • weekend
<0-23> <0-59>	After specifying the start day, specify the start time in hours (24 hours format) and minutes • <0-23> – Specify the start time from 0 - 23 hours. • <0-59> – Specify the start time from 0 - 59 minutes. For example, if the values provided are 12 hours and 30 minutes, the start time is 12:30 A.M on the specified day.
to [<023> <0-59>|daily| friday|monday| saturday| sunday| thursday|tuesday| wednesday| weekdays| weekend]	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: • <0-23> <0-59> – 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. • daily – Select this option if the time range starts and ends every day at a specified time • friday – Select this option if the time range ends on Fridays • monday – Select this option if the time range ends on Mondays • saturday – Select this option if the time range ends on Saturdays • sunday – Select this option if the time range ends on Sundays • thursday – Select this option if the time range ends on Thursdays • tuesday – Select this option if the time range ends on Tuesdays • wednesday – Select this option if the time range ends on Wednesdays • weekdays – Select this option if the time range ends on Weekdays • weekend – Select this option if the time range ends on Weekends 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.
<0-23> <0-59>	After specifying the end day, specify the end time in hours (in 24 hours format) and minutes • <0-23> – Specify the end time from 0 - 23 hours. • <0-59> – Specify the end minute from 0 - 59 minutes. 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.
rule-precedence <1-7>	Configures a precedence value for this periodic time range rule. Rules with lower precedence have higher priority and are applied first. • <1-7> – Specify a precedence value from 1 - 7.

Examples

```
EX3500(config-ex3500-time-range-EX3500-TimeRange-01)#periodic daily 1 10
to daily 23 10 rule-precedence 1

EX3500(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
EX3500(config-ex3500-time-range-EX3500-TimeRange-01)#
```

Related Commands

no (ex3500-time-range-config-mode) on page 317	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 7500, NX 95XX, NX 96XX

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>
```

no <PARAMETERS>	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 EX3548 profile, which is then applied to an adopted EX3500 series switch.

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.

Going forward NX7500, NX9500, and NX9600 WiNG managed series service platforms and 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 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 — NZ7500, NX9500, NX9600, VX9000

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)#?
nx9500-6C8809_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

no on page 611	Removes this EX3500 management policy

ex3500-management-policy-config-commands

Table 14: EX3500 Management Policy Config Commands

Command	Description
enable on page 319	Configures an executive password for this EX3500 management policy
http on page 320	Configures the HTTP server settings used to authenticate HTTP connection to a EX3500 switch
memory on page 321	Configures the EX3500's memory utilization rising (upper) and falling (lower) threshold values
process-cpu on page 322	Configures the EX3500's CPU (processor) utilization rising (upper) and falling (lower) threshold values
snmp-server on page 323	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.
ssh on page 330	Configures the SSH server settings used to authenticate SSH connection to a EX3500 switch
username on page 331	Configures a EX3500 switch user settings
no (ex3500-management-policy-config-mode) on page 332	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 96XX, 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] <PASSWORD>	Creates a new executive password for this EX3500 management policy. The password could be in clear text or encrypted • 0 – Configures a clear text password using ASCII characters (should be 1 - 32 characters long) • 7 – Configures an encrypted password using HEX characters (should be 32 characters long) • <PASSWORD> – Specify the password.

```
enable password level <0-15> [0 <PASSWORD>|7 <PASSWORD>]
```

enable password level <0-15>	Creates a new executive password for this EX3500 management policy and sets its privilege level • <0-15> – 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.
[0|7] <PASSWORD>	After setting the privilege level, configure the password, which could be in clear text or encrypted • 0 – Configures a clear text password using ASCII characters (should be 1 - 32 characters long) • 7 – Configures an encrypted password using HEX characters (should be 32 characters long) • <PASSWORD> – Specify the password.

Examples

```
nx9500-6C8809(config-ex3500-management-policy-test)#enable password level 3 7
1234567890102030405060708092929l
nx9500-6C8809(config-ex3500-management-policy-test)#show context
ex3500-management-policy test
 enable password level 3 7 1234567890102030405060708092929l
 snmp-server notify-filter 1 remote 127.0.0.1
nx9500-6C8809(config-ex3500-management-policy-test)#
```

Related Commands

no (ex3500-management-policy-config-mode) on page 332	Removes a executive password from this EX3500 management policy

http

Configures the HTTP server settings used to authenticate HTTP 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 un-used 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 96XX, NX 7510

Syntax

```
http [port <1-65535>|secure-port <1-65535>|secure-server|server]
```

Parameters

```
http [port <1-65535>|secure-port <1-65535>|secure-server|server]
```

http	Configures following HTTP settings: port, secure-port, secure-server, and server
port <1-65535>	Configures the HTTP port number. This is the port used to connect to the HTTP server. • <1-65535> – Specify a value from 1 - 65535. The default port is 80.
secure-port <1-65535>	Enables secure HTTP connection over a designated secure port. Ensure that the HTTP secure server is enabled before specifying the secure-server port. • <1-65535> – Specify the secure HTTP server port from 1 - 65535. The default port is 443.
secure-server	Enables HTTP secure server. This option is disabled by default.
server	Enables HTTP server. This option is enabled by default. Consequently, HTTP management access is allowed by default.

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 (ex3500-management-policy-config-mode) on page 332	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 96XX, 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 • <1-100> – Specify the falling threshold as a percentage from 1 - 100. The default is 70%.
rising-threshold <1-100>	Configures the rising threshold for the EX3500's memory utilization • <1-100> – Specify the rising threshold as a percentage from 1 - 100. The default is 90%.

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

no (ex3500-management-policy-config-mode) on page 332	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 96XX, 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 • <1-100> – Specify the falling threshold as a percentage from 1 - 100. The default is 70%.
rising-threshold <1-100>	Configures the rising threshold for the EX3500's CPU utilization • <1-100> – Specify the rising threshold as a percentage from 1 - 100. The default is 90%.

Example

```
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 (ex3500-management-policy-config-mode) on page 332	Reverts the CPU utilization's falling-threshold and/or rising threshold to 70% and 90% respectively

snmp-server

Configures *Simple Network Management Protocol* (SNMP) 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 96XX, 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}}
```

snmp-server {community <STRING> {ro|rw}}	Configures SNMP-server related settings • community – Optional. Configures an SNMP community access string used to authorize management access by clients using SNMP v1, v2c, or v3 • <STRING> – Specify the SNMP community access string (should not exceed 32 characters). After specifying the string, optionally specify the access type associated with it. • 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. • rw – Optional. Provides read-write access with this SNMP community string. Allows authorized clients to retrieve as well as modify MIB objects. You can configure a maximum of five (5) community strings per vEX3500 management policy.

```
snmp-server {contact <NAME>}
```

snmp-server {contact <NAME>}	Configures SNMP-server related settings • contact – Optional. Configures the system's contact information • <NAME> – Specify the contact person's name (should not exceed 255 characters).

```
snmp-server {enable traps {authentication|link-up-down}}
```

snmp-server {enable traps {authentication|link-up-down}}	Configures SNMP-server related settings
	• enable traps – Optional. Enables the EX3500 switch to send following SNMP traps or notifications:
	  • authentication – Optional. Enables SNMP authentication trap. This option is disabled by default.
	  • link-up-down – Optional. Enables SNMP link up and link down traps. This option is disabled by default.
	If the command is executed without either of the above mentioned trap options, the system enables both authentication and link-up-down traps.
	If enabling SNMP traps, use the `snmp-server > host` command to specify the host(s) receiving the SNMP notifications.

```
snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}
```

snmp-server {engine-id [local <WORD>|remote <IP> <WORD>]}	Configures SNMP-server related settings
	• 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.
	  • local – Configures the SNMP engine on the logged switch
	  <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).
	  • remote <IP> <WORD> – Configures a remote device as the SNMP engine
	  <IP> – Specify the remote device's IP address.
	  <WORD> – Specify the hexadecimal engine ID string identifying the SNMP engine (should be 9 - 64 characters in length).
	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.

```
snmp-server {group <GROUP-NAME> [v1|v2c|v3 [auth|noauth|priv]] {notify <WORD>|
read <WORD>|write <WORD>}}
```

snmp-server group <GROUP-NAME>	Configures SNMP-server related settings • group – Optional. Configures an SNMP user group, mapping SNMP users to SNMP views • <GROUP-NAME> – Specify the SNMP group name (should not exceed 32 characters).

[v1|v2c|v3 [auth|noauth|priv]]	Configures the SNMP version used for authentication by this user group
	• v1 – Configures the SNMP version as v1.
	• v2c – Configures SNMP version as v2c
	• v3 – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.
	  • auth – Uses SNMP v3 with authentication and no privacy
	  • noauth – Uses SNMP v3 with no authentication and no privacy
	  • priv – Uses SNMP v3 with authentication and privacy

notify <WORD>	Optional. Configures the notification view string • <WORD> – Specify the string (should not exceed 32 characters).
read <WORD>	Optional. Configures the read view string • <WORD> – Specify the string (should not exceed 32 characters).
write <WORD>	Optional. Configures the write view string • <WORD> – Specify the string (should not exceed 32 characters).

```
snmp-server {host <IP> <STRING> version [v1|v2c|v3 [auth|noauth|priv]] {udp-port
<1-65535>}}
```

snmp-server host <IP>	Configures SNMP-server related settings • 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 • <IP> – Specify the SNMP host's IP address. You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy. Ensure that SNMP trap notification is enabled.
<STRING>	Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the `snmp-server > community <STRING> > {ro|rw}` command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host. • <STRING> – Specify the community string. The string configured here is sent in the SNMP traps to the SNMPv1 or SNMPv2c hosts.
version [v1|v2c| v3 [auth| noauth| priv]]	Configures the SNMP version used • v1 – Configures the SNMP version as 1. This is the default setting. • v2c – Configures SNMP version as 2c • v3 – Configures the SNMP version as 3. If using SNMPv3, specify the authentication and encryption levels. • auth – Uses SNMP v3 with authentication and no privacy • noauth – Uses SNMP v3 with no authentication and no privacy • priv – Uses SNMP v3 with authentication and privacy
udp-port <1-65535>	Optional. After specifying the SNMP version, optionally specify the host UDP port • <1-65535> – Specify the UDP port. The default is 162.

```
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>	Configures SNMP-server related settings • host – Optional. Configures the host(s) receiving the SNMP notifications • <IP> – Specify the SNMP host's IP address. You can configure a maximum of five (5) SNMP trap recipients per EX3500 management policy. Ensure that SNMP trap notification is enabled.
inform [retry <0-255>| timeout <0-2147483647>]	Enables sending of SNMP notifications as inform messages, and configures inform message settings. • retry <0-255> – Configures the maximum number attempts made to re-send an inform message in case the specified SNMP host does not acknowledge receipt. <0-255> – Specify a value from 0 - 255. The default is 3. • timeout <0-2147483647> – Configures the interval, in seconds, to wait for an acknowledgment from the SNMP host before re-sending an inform message • <0-2147483647> – Specify a value from 0 - 2147483647 seconds. The default is 1500 seconds. 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.
<STRING>	Configures the SNMP community string. You can configure the SNMP community string here, or else use the string configured using the `snmp-server > community <STRING> > {ro|rw}` command. It is recommended that you configure the SNMP community string prior to configuring the SNMP host. • <STRING> – Specify the community string. The string configured here is sent in the SNMP inform messages to the SNMPv2c or SNMPv3 hosts.

version [v2c| v3 [auth|noauth| priv]]	Configures the SNMP version used
	• v2c – Configures the SNMP version as v2c
	• v3 – Configures the SNMP version as v3. If using SNMP v3, specify the authentication and encryption levels.
	  • auth – Uses SNMP v3 with authentication and no privacy
	  • noauth – Uses SNMP v3 with *no authentication* and *no privacy*
	  • priv – Uses SNMP v3 with authentication and privacy
	
	SNMP inform messages are not supported on SNMP v1.

udp-port <1-65535>	Optional. After specifying the SNMP version, optionally specify the host UDP port • <1-65535> – Specify the UDP port. The default is 162.

```
snmp-server {location <WORD>}
```

snmp-server {location <WORD>}	Configures SNMP-server related settings • location – Optional. Configures the EX3500's location string • <WORD> – Specify the location (should not exceed 255 characters).

```
snmp-server {notify-filter <WORD> remote <IP>}
```

snmp-server notify-filter <WORD>	Configures SNMP-server related settings • notify-filter – Optional. Modifies the SNMP server's notify filter • <WORD> – Specify the SNMP notify-filter name.
remote <IP>	Optional. Configures the remote host's IP address • <IP> – Specify the IP address in the A.B.C.D format.

```
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 • 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. • <USER-NAME> – Specify the user's name (should not exceed 32 characters). <GROUP-NAME> – Specify the SNMP group name to which this user is assigned.
remote <IP> v3	Configures the remote host on which the SNMPv3 engine is running • <IP> – Specify the remote host's IP address. This option is available only for SNMPv3 engine. After configuring the remote host, optionally configure the authentication type and the corresponding authentication password used.
{auth|encrypted auth} [md5| sha] <WORD> {priv [3des| aes128| aes192|aes256| des56] <WORD>}	Optional. Configures authentication and encryption settings • auth – Specifies the authentication type used and configures the authentication password • 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. The following parameters are common to the 'auth' and 'encrypted' keywords: • md5 – Uses MD5 to authenticate the user • sha – Uses SHA to authenticate the user The following parameter is common to the 'md5' and 'sha' keywords: • <WORD> – Specify the authentication password. 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. • priv – Optional. Uses SNMPv3 with privacy. Select one of the privacy options: des, aes128, aes192, aes256, des56. • <WORD> – 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.

```
snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}
```

snmp-server {user <USER-NAME> <GROUP-NAME> [v1|v2c|v3]}	Configures SNMP-server related settings • 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. • <USER-NAME> – Specify the user's name (should not exceed 32 characters). <GROUP-NAME> – Specify the SNMP group name to which this user is assigned. [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. 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.

```
snmp-server {view <VIEW-NAME> <OID-TREE-STRING> [excluded|included]}
```

snmp-server view <VIEW-NAME>	Configures SNMP-server related settings • view – Optional. Creates an SNMP view. SNMP views are used to control user access to the MIB. • <VIEW-NAME> – Provide a name for this SNMP view (should not exceed 32 characters).
<OID-TREE-STRING> [excluded|included]	Configures the *object identifier* (OID) of a branch within the MIB tree • excluded – Specifies an excluded view • included – Specifies an included view

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
snmpteststring 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 snmpteststring 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

no (ex3500-management-policy-config-mode) on page 332	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 96XX, 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 • <1-5> – Specify a value from 1 - 5. The default setting is 3.
server	Enables SSH server connection
server-key size <512-1024>	Configures the SSH server key size • <512-1024> – Specify the SSH server key from 512 - 1,024. The default length is 768.
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. • <1-120> – Specify a value from 1 120 seconds. The default is 120 seconds.

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 (ex3500-management-policy-config-mode) on page 332	Disables SSH management access to an EX3500 switch

username

Configures a vEX3500 switch user settings

The EX3500 switch user details are stored in a local database on the NX 95XX, NX 96XX, 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 96XX, 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 • <USER-NAME> – Specify the user name (should not exceed 32 characters)
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. • <0-15> – Specify the access level from 0 - 15. The default is 0.
nopassword	Allows user to login without a password
password [0|7] <PASSWORD>	Configures the password for this user • 0 – Configures a plain text password • 7 – Configures an encrypted password (should be 32 characters in length) • <PASSWORD> – Specify the password.

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 1234567890102030405060708092929l
 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 (ex3500-management-policy-config-mode) on page 332	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 96XX, 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 snmpteststring 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 snmpteststring 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 — NX7500, NX9500, NX9600, VX9000

Syntax

```
ex3500-qos-class-map-policy <POLICY-NAME>
```

Parameters

```
ex3500-qos-class-map-policy <POLICY-NAME>
```

<POLICY-NAME>	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

no on page 611	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 15: EX3500 QoS Class Map Policy Config Commands

Command	Description
description on page 334	Configures a description for this EX3500 QoS class map policy
match on page 335	Configures match criteria rules used to classify traffic
rename on page 337	Renames an existing EX3500 QoS class map object
no (ex3500-qos-class-map-policy-config-commands) on page 337	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 7510, NX 95XX, NX 96XX

Syntax

```
description <LINE>
```

Parameters

```
description <LINE>
```

description <LINE>	Configures this EX3500 QoS class map policy'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-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

no (ex3500-qos-class-map-policy-config-commands) on page 337	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 7510, NX 95XX, NX 96XX

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	Configures the match criteria. The options are: access-list, cos, ip, ipv6, vlan Incoming packets matching the specified criteria are included in this QoS class map.
access-list [ex3500-ext-access-list| ex3500-std-access-list| mac-acl] <ACL-NAME>	Uses access lists to provide the match criteria. You can use any one the following ACL types to classify traffic: • ex3500-ext-access-list – Uses an IPv4 EX3500 extended ACL • ex3500-std-access-list – Uses an IPv4 EX3500 standard ACL • mac-acl – Uses a MAC EX3500 ACL The following keyword is common to all of the above ACL types: • <ACL-NAME> – Specify the ACL name (should be existing and configured).

cos <0-7>	Configures the *class of service* (CoS) 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. • <0-7> – Specify the CoS value from 0 - 7. Following are the 8 traffic classes based on the CoS value: • 000 (0) - Routine • 001 (1) - Priority • 010 (2) - Immediate • 011 (3) - Flash • 100 (4) - Flash Override • 101 (5) - Critical • 110 (6) - Internetwork Control • 111 (7) - Network Control
ip [dscp <0-63>| precedence <0-7>]	Configures the IPv4 DSCP value to match and/or the IP precedence value to match. • <0-63> – Specify the DSCP value from 0 - 63. Use this option to specify the *type of service* (ToS) 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. • precedence <0-7> – Configures the IP precedence to match. Following are the 8 traffic classes based on the IP precedence values: • 000 (0) - Routine • 001 (1) - Priority • 010 (2) - Immediate • 011 (3) - Flash • 100 (4) - Flash Override • 101 (5) - Critical • 110 (6) - Internetwork Control • 111 (7) - Network Control
ipv6 dscp <0-63>	Configures the IPv6 DSCP value to match • <0-63> – Specify the DSCP value from 0 - 63.
vlan <1-4094>	Configures the VLAN to match • <1-4094> – Specify the VLAN ID.

Usage Guidelines

When configuring match entries, take into consideration the following points:

- Deny rules included in an ACL (associated with a vEX3500 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 (ex3500-qos-class-map-policy-config-commands) on page 337	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 7510, NX 95XX, NX 96XX

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 • <EX3500-QOS-CLASS-MAP-POLICY-NAME> – Enter the EX3500 QoS class map's current name. • <NEW-EX3500-QOS-CLASS-MAP-POLICY-NAME> – Enter the new name.

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 (ex3500-qos-class-map-policy-config-commands)

description

Removes this EX3500 QoS class map policy's description and match criteria

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX

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. Create a 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 on page 335.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

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)#?
nx9500-6C8809_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 on page 611	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 16: EX3500 QoS Policy Map Config Commands

Command	Description
class on page 339	Creates a policy map class and enters its configuration mode
description on page 347	Configures this EX3500 QoS policy map's description
no (ex3500-qos-policy-map) on page 348	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 7510, NX 95XX, NX 96XX

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

set on page 345	Sets CoS value, *per-hop behavior* (PHB) value, and IP DSCP value in matching packets
police on page 340	Configures an enforcer for classified traffic
no (ex3500-qos-policy-map) on page 348	Removes this traffic classification's settings

police

Configures an enforcer for classified traffic

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX

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> <0-16000000>	Configures an enforcer for classified traffic based on the metered flow rate • <0-1000000> – Configures the CIR *(committed information rate)* from 0 -1000000 kilobits per second. • <0-16000000> – Configures the BC *(committed burst size)* from 0 - 16000000 bytes. 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. The behavior of the meter is specified in terms of one *token bucket* (C), the rate at which the tokens are incremented CIR and the maximum size of the token bucket BC. The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:
conform-action transmit	Configures the action applied when packets fall within the specified CIR and BC limits • 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.
violate-action [<0-63>|drop]	Configures the action applied when packets violate the specified CIR and BC limits • <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63. • drops – Drops packets violating the specified CIR and BC limits

```
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>	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)*. • srtcm-color-blind - Single rate three color meter in color-blind mode • srtcm-color-aware - Single rate three color meter in color-aware mode 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. • <0-1000000> – Configures the CIR from 0 -1000000 kilobits per second. • <0-16000000> – Configures the BC from 0 - 1600000 bytes. <0-16000000> – Configures the BE from 0 - 1600000 bytes. 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 Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows: • If Tc is less than BC, Tc is incremented by one, else • If Te is less then BE, Te is incremented by one, else • neither Tc nor Te is incremented. When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode: • If Tc(t)-B > OR = 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else • if Te(t)-B > OR = 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, • else the packet is red and neither Tc nor Te is decremented. When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode: • If the packet has been pre-colored as green and Tc(t)-B 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else • If the packet has been pre-colored as yellow or green and if • Te(t)-B > OR = 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented. 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.
conform-action transmit	Configures the action applied when packet rates fall within the specified CIR and BC limits • transmit – Transmits packets falling within the specified CIR and BC limits

exceed-action [<0-63>|drop]	Configures the action applied when packet rates exceed the specified CIR and BC limits • <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63 • drops – Drops packets exceeding the specified CIR and BC limits
violate-action [<0-63>|drop]	Configures the action applied when packet rates exceed the specified BE limit • <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63 • drops – Drops packets exceeding the specified BE limit

```
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>	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 *Peak Information Rate* (PIR), and their associated burst sizes - BC and BP *(Peak Burst Size)*. • trtcm-color-blind - Two rate three color meter in color-blind mode • trtcm-color-aware - Two rate three color meter in color-aware mode • <0-1000000> – Configures the CIR from 0 - 1000000 kilobits per second <0-16000000> – Configures the BC from 0 - 1600000 bytes. <0-1000000> – Configures the PIR from 0 - 1000000 kilobits per second <0-16000000> – Configures the BP from 0 - 1600000 bytes 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. 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 Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC. When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode: • If Tp(t)-B < 0, the packet is red, else • if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else • The packet is green and both Tp and Tc are decremented by B. When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode: • If the packet has been pre-colored as red or if Tp(t)-B < 0, the packet is red, else • if the packet has been pre-colored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else • the packet is green and both Tp and Tc are decremented by B. 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.
conform-action transmit	Configures the action applied when packet rates fall within the specified CIR and BP limits • transmit – Transmits packets falling within the specified CIR and BC limits

exceed-action [<0-63>| drop]	Configures the action applied when packet rates exceed the specified CIR limit, but are within the specified PIR limit • <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63. • drops – Drops packets exceeding the specified CIR and BC limit
violate-action [<0-63>| drop]	Configures the action applied when packet rates exceed the specified PIR limit • <0-63> – Applies a new DSCP value. Select the DSCP value from 0 - 63. • drops – Drops packets exceeding the specified BE limi

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

no (ex3500-traffic-class-config-commands) on page 347	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 7510, NX 95XX, NX 96XX

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 • <0-7> – Specify a value from 0 - 7. The CoS is modified to the value specified here.
ip dscp <0-63>	Modifies the IP DSCP value in a matching packet (as specified by the match command) • <0-63> – Specify a value from 0 - 63. The DSCP value is modified to the value specified here.
phb <0-7>	Configures a PHB value for a matching packets • <0-7> – Specify a value from 0 -7. 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: • green if it does not exceed the CIR and BC limits • yellow if it exceeds the CIR and BC limits, but not the BE limit, and • red otherwise.

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 (ex3500-traffic-class-config-commands) on page 347	Removes CoS value, PHB value, or IP DSCP value from this traffic class

no (ex3500-traffic-class-config-commands)

Removes this traffic classification's settings

Supported in the following platforms:

- Service Platforms — NX 7510, NX 95XX, NX 96XX

Syntax

```
no [police|set]
no police [flow|srtcm-color-aware|srtcm-color-blind|trtcm-color-aware|trtcm-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 7510, NX 95XX, NX 96XX

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 (ex3500-qos-policy-map) on page 348	Removes this EX3500 QoS policy map's description

no (ex3500-qos-policy-map)

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 7510, NX 95XX, NX 96XX

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)#
EX3500(config-ex3500-qos-policy-map-test)#no description
EX3500(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:

```
EX3500(config-ex3500-qos-policy-map-test)#show context
ex3500-qos-policy-map test
EX3500(config-ex3500-qos-policy-map-test)#
```

ex3524

Adds a EX3524 switch to the network

The EX3524 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 switch's device configuration mode and execute the following command: `controller > host > <IP/HOSTANME>`.

EX3524 devices 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 EX3524 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3524 switch utilizes an embedded HTTP Web agent and CLI, which in spite of being different from that of the EX3524 operating system provides EX3524 controllers PoE and port management resources.

Going forward NX7500, NX9500, and NX9600 series service platforms and WiNG VMs can discover, adopt, and partially manage EX3524 series Ethernet switches without modifying the proprietary operating system running the EX3524 switches. The WiNG service platforms utilize standardized WiNG interfaces to push configuration files to the EX3524 switches, and maintain a translation layer, understood by the EX3524 switch, for statistics retrieval.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes a EX3524 switch from the network

ex3548

Adds a EX3548 switch to the network

The EX3548 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 — NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes a EX3548 switch from the network

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing event system policy

event-system-policy-mode-commands

The following table summarizes event system policy configuration mode commands:

Table 17: Event-System-Policy Config Mode Commands

Command	Description
event on page 352	Configures an event
no (event-system-policy-config-mode) on page 366	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
  bonjgw           Bonjgw 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
  dhcpsvr          DHCP Configuration Daemon
  diag             Diag module
  dot11            802.11 management module
  dot1x            802.1X Authenticationn
  fa               Fabric Attach
  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         Smtpnot module
  system          System module
  test            Test module
  tron            TRON Feature
  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: • radius-discon-msg – RADIUS disconnection message • radius-session-expired – RADIUS session expired message • radius-session-not-started – RADIUS session not started message • radius-vlan-update – RADIUS VLAN update message
adapt	Enables and configures logging of the following adaptivity module related events: • adaptivity-change – Event adaptivity change • adaptivity-rehome – Event adaptivity rehome
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: • adopted – Event AP adopted • adopted-to-controller – Event AP adopted to wireless controller • ap-adopted – Event access port adopted • ap-autoup-done – Event AP autoup done • ap-autoup-fail – Event AP autoup fail • ap-autoup-needed – Event AP autoup needed • ap-autoup-no-need – Event AP autoup not needed • ap-autoup-reboot – Event AP autoup reboot • ap-autoup-timeout – Event AP autoup timeout • ap-autoup-ver – Event AP autoup version • ap-reset-detected – Event access port reset detected • ap-reset-request – Event access port user requested reset • ap-timeout – Event access port timed out • ap-unadopted – Event access port unadopted • image-parse-failure – Event image parse failure • legacy-auto-update – Event legacy auto update • no-image-file – Event no image file • offline – Event AP detected as offline • online – Event offline AP detected as online • reset – Event reset • sw-conn-lost – Event software connection lost • unadopted – Event unadopted
bt	Enables and configures logging of the following bluetooth related events: • bt-started – Event bluetooth (bt) started • bt-state-change – Event bt state change • bt-tron-license - Logs a TRON license exists event • bt-tron-no-license - Logs a TRON license missing event
captive-portal	Enables and configures logging of the following captive portal (hotspot) related events: • allow-access – Event client allowed access • auth-failed – Event client authentication failed • auth-success – Event client authentication success • client-disconnect – Event client disconnected • client-removed – Event client removed • data-limit-exceed – Event client data limit exceeded • flex-log-access – Event flexible log access granted to client • inactivity-timeout – Event client time-out due to inactivity • page-cre-failed – Event page creation failure • purge-client – Event client purged • session-timeout – Event session timeout • vlan-switch – Event client switched VLAN

<event-type>	<event-name>
cdp	Enables and configures logging of the following *CISCO Discovery Protocol* (CDP) related event: • duplex-mismatch – Event duplex mismatch detected between CDP neighbors
certmgr	Enables and configures logging of the following certificate manager related events: • ca-cert-actions-failure – Event CA certificate actions failure • ca-cert-actions-success – Event CA certificate actions success • ca-key-actions-failure – Event CA key actions failure • ca-key-actions-success – Event CA key actions success • cert-expiry – Event certificate expiry • crl-actions-failure – Event *Certificate Revocation List* (CRL) actions failure • crl-actions-success – Event CRL actions success • csr-export-failure – Event CSR export failure • csr-export-success – Event CSR export success • delete-trustpoint-action – Event delete trustpoint action • export-trustpoint – Event trustpoint exported • import-trustpoint – Event trustpoint imported • rsa-key-actions-failure – Event RSA key actions failure • rsa-key-actions-success – Event RSA key actions success • svr-cert-actions-success – Event server certificate actions success • svr-cert-actions-failure – Event server certificate actions failure
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: • acl-attached-altered – Event *Access List* (ACL) attached altered • acl-rule-altered – Event ACL rule altered
cluster	Enables and configures logging of the following cluster module related events: • cmaster-cfg-update-fail – Event cluster master config update failed • max-exceeded – Event maximum cluster count exceeded • state-change – Event cluster state change (active/inactive) • state-change-active – Event cluster state change to active • state-change-inactive – Event cluster state change to inactive • state-retain-active – Event cluster state retained as active
crm	Enables and configures logging of the following *Critical Resource Monitoring* (CRM) related event • critical-resource-down – Event critical resource goes down • critical-resource-up – Event critical resource comes up
device	Enables and configures the logging of device module related events

<event-type>	<event-name>
database	Enables and configures logging of the following error conditions in the captive-portal/NSIght database: • database-election-fail – Event primary database node selection failure. Requires manual intervention to select primary database node. • database-exception – Event database may need to be dropped and device restarted • database-low-disk-space – Event database low disk space • database-new-state – Event database state change • database-op-failure – Event database failure • database-set-name-mismatch – Event replica-set not enabled on host • database-storage-mismatch – Event database mismatch. All database files must be removed. • operation-complete – Event database operation completed successfully • operation-failed – Event database operation failure
dhcpsvr	Enables and configures logging of the following DHCP server related events: • dhcp-start – Event DHCP server started • dhcpsvr-stop – Event DHCP sever stopped • relay-iface-no-ip – Event no IP address on DHCP relay interface • relay-no-iface – Event no interface for DHCP relay • relay-start – Event relay agent started • relay-stop – Event DHCP relay agent stopped

<event-type>	<event-name>
diag	Enables and configures logging of the following diagnostics module related events: • autogen-tech-sprt – Event autogen technical support • buf-usage – Event buffer usage • cpu-load – Event CPU load • cpu-usage-too-high – Event CPU usage high • cpu-usage-too-high-recovery – Event recovery from high CPU usage • disk-usage – Event disk usage • elapsed-time – Event elapsed time • fan-underspeed – Event fan underspeed • fd-count – Event forward count • free-flash-disk – Event free flash disk • free-flash-inodes – Event free flash inodes • free-nvram-disk – Event free nvram disk • free-nvram-inodes – Event free nvram inodes • free-ram – Event free ram • free-ram-disk – Event free ram disk • free-ram-inodes – Event free ram inodes • head-cache-usage – Event head cache usage • high-temp – Event high temp • ip-dest-usage – Event ip destination usage • led-identify – Event led identify • low-temp – Event low temp • mem-usage-too-high – Event memory usage high • mem-usage-too-high-recovery – Event recovery from high memory usage • new-led-state – Event new led state • over-temp – Event over temp • over-voltage – Event over voltage • poe-init-fail – Event PoE init fail • poe-power-level – Event PoE power level • poe-read-fail – Event PoE read fail • poe-state-change – Event PoE state change • poe-state-change – Event PoE state change • pwrsply-fail – Event failure of power supply • raid-degraded – Event *Redundant Array of Independent Disks* (RAID) degraded • raid-error – Event RAID error • ram-usage – Event ram usage • under-voltage – Event under voltage • wd-reset-sys – Event wd reset system • wd-state-change – Event wd state change

<event-type>	<event-name>
dot11	Enables and configures logging of the following 802.11 management module related events: • client-assoc-ignored – Wireless client association ignored event • client-associated – Wireless client associated event • client-denied-assoc – Event client denied association • client-disassociated – Wireless client disassociated • country-code – Event country code applied • country-code-error – Event country code error • eap-cached-keys – Event *Extensible Authentication Protocol* (EAP) cached keys • eap-client-timeout – Event EAP client timeout • eap-failed – Event EAP failed • eap-opp-cached-keys – Event EAP opp cached keys • eap-preauth-client-timeout – Event EAP pre authentication client timeout • eap-preauth-failed – Event EAP pre authentication failed • eap-preauth-server-timeout – Event EAP pre authentication server timeout • eap-preauth-success – Event EAP pre authentication success • eap-server-timeout – Event EAP server timeout • eap-success – Event EAP success • ft-roam-success – Event client fast BSS transition • gal-rx-request – Event GAL request received event • gal-tx-response – Event response sent to GAL request • gal-validate-failed – Event GAL validation failed • gal-validate-req – Event GAL validation request • gal-validate-success – Event GAL validation success • kerberos-client-success – Event client Kerberos authentication success • kerberos-wlan-failed – Event WLAN Kerberos authentication failed • kerberos-wlan-success – Event WLAN Kerberos authentication success • kerberos-wlan-timeout – Event Kerberos authentication timed out • move-operation-success – Event move operation success • tkip-cntrmeas-end – Event TKIP countermeasures ended • tkip-cntrmeas-start – Event TKIP countermeasures initiated • tkip-mic-fail-report – Event TKIP MIC failure report • tkip-mic-failure – Event TKIP MIC check failed • neighbor-denied-assoc – Event neighbor denied association • unsanctioned-ap-active – Event unsanctioned AP active • unsanctioned-ap-inactive – Event unsanctioned AP inactive • unsanctioned-ap-status-change – Event unsanctioned AP status change • voice-call-completed – Event voice call completed • voice-call-established – Event voice call established • voice-call-failed – Event voice call failed • wlan-time-access-disable – Event WLAN disabled by time-based-access • wlan-time-access-enable – Event WLAN re-enabled by time-based-access

<event-type>	<event-name>
	• wpa-wpa2-failed – Event WPA-WPA2 failed • wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn • wpa-wpa2-success – Event WPA-WPA2 success
dot1x	Enables and configures logging of the following 802.1X authentication related events: • dot1x-failed – Event EAP authentication failure • dot1x-success – Event dot1x-success
fa	Enables and configures logging of fabric attach related events: • fa-accepted – Event fa-accepted • fa-pending – Event fa-pending
fwu	Enables and configures logging of the following *firmware update* (FWU) related events: • fwuaborted – Event fwu aborted • fwubadconfig – Event fwu aborted due to bad config • fwucorruptedfile – Event fwu aborted due to corrupted file • fwucouldntgetfile – Event fwu aborted because the system could not get file • fwudone – Event fwu done • fwufileundef – Event fwu aborted due to file undefined • fwunoneed – Event fwu no need • fwuprodmismatch – Event fwu aborted due to product mismatch • fwuserverundef – Event fwu aborted due to server undefined • fwuserverunreachable – Event fwu aborted due to server unreachable • fwusignmismatch – Event fwu aborted due to signature mismatch • fwusyserr – Event fwu aborted due to system error • fwuunsupportedhw – Event fwu aborted due to unsupported hardware • fwuunsupportedmodelnum – Event fwu aborted due to unsupported FIPS model number • fwuvermismatch – Event fwu aborted due to version mismatch
isdn	Configures file *Integrated Service Digital Network* (ISDN) module related event s • isdn-alert – Event ISDN alert • isdn-crit – Event ISDN critical • isdn-debug – Event ISDN debug • isdn-emerg – Event ISDN emergency • isdn-err – Event ISDN error • isdn-info – Event ISDN info • isdn-notice – Event ISDN notice • isdn-warning – Event ISDN warning
l2gre	Enables and configures logging of the following *Layer 2 GRE* (L2GRE) tunnel related events: • l2gre-tunnel-down – Event L2GRE tunnel down • l2gre-tunnel-failover – Event L2GRE tunnel failover • l2gre-tunnel-up – Event L2GRE tunnel up

<event-type>	<event-name>
l2tpv3	Enables and configures logging of the following *Layer 2 TPV3* (L2TPv3) tunnel related events: • l2tpv3-tunnel-down – Event L2TPv3 tunnel down • l2tpv3-tunnel-up – Event L2TPv3 tunnel up
licmgr	Enables and configures logging of the following license manager module related events: • lic-installed-count – Event total number of license installed count • lic-installed-default – Event default license installation • lic-installed – Event license installed • lic-invalid – Event license installation failed • lic-removed – Event license removed
lldp	Enables and configures logging of the following *Link Layer Discovery Protocol* (LLDP) related events: • lldp-loop-detected – Event layer 2 switching loop • lldp-loop-recovery – Event recovery from layer 2 switching loop
mgmt	Enables and configures logging of the following management services module related events: • log-http-init – Event Web server started • log-http-local-start – Event Web server started in local mode • log-http-start – Event Web server started in external mode • log-https-start – Event secure Web server started • log-https-wait – Event waiting for Web server to start • log-key-deleted – Event RSA key associated with SSH is deleted • log-key-restored – Event RSA key associated with SSH is added • log-trustpoint-deleted – Event trustpoint associated with HTTPS is deleted
mesh	Enables and configures logging of the following mesh module related events: • mesh-link-down – Event mesh link down • mesh-link-up – Event mesh link up • meshpoint-down – Event meshpoint down • meshpoint-loop-prevent-off – Event meshpoint loop prevent off • meshpoint-loop-prevent-on – Event meshpoint loop prevent on • meshpoint-path-change – Event meshpoint-path-change • meshpoint-root-change – Event meshpoint-root-change • meshpoint-up – Event meshpoint up

<event-type>	<event-name>
nsm	Configures *Network Service Module* (NSM) related event • dhcpc-err – Event DHCP certification error • dhcpdefrt – Event DHCP defrt • dhcpip – Event DHCP IP • dhcpipchg – Event DHCP IP change • dhcpipnoadd – Event DHCP IP overlaps static IP address • dhcplsexp – Event DHCP lease expiry • dhcpnak – Event DHCP server returned DHCP NAK response • dhcpnodefrt – Event interface no default route • if-failback – Event interface failback • if-failover – Event interface failover • ifdown – Event interface down • ifipcfg – Event interface IP config • ifup – Event interface up • nsm-ntp – Event translate host name
pm	Configures process monitor module related event s • procid – Event proc ID generated • procmaxrstrt – Event proc max restart • procnoresp – Event proc no response • procrstrt – Event proc restart • procstart – Event proc start • procstop – Event proc stop • procsysrstrt – Event proc system restart • startupcomplete – Event startup complete
radconf	Enables and configures logging of the following RADIUS configuration daemon related events: • could-not-stop-radius – Event could not stop RADIUS server • radiusdstart – Event RADIUS server started • radiusdstop – Event RADIUS server stopped

<event-type>	<event-name>
radio	Enables and configures logging of the following radio module related events: • acs-scan-complete – Event ACS scan completed • acs-scan-started – Event ACS scan started • cb-associated – Event client-bridge access point associates with an infrastructure access point • cb-roam – Event client-bridge access point roams from one infrastructure access point to another infrastructure access point • cb-wired-client-added – Event wired client is added to the client-bridge • cb-wired-client-removed – Event wired client is removed from the client-bridge • channel-country-mismatch – Event channel and country of operation mismatch • radar-det-info – Detected radar info • radar-detected – Event radar detected • radar-scan-completed – Event radar scan completed • radar-scan-started – Event radar scan started • radio-antenna-error – Event invalid antenna type on this radio • radio-antenna-setting – Event antenna type setting on this radio • radio-state-change – Event radio state change • resume-home-channel – Event resume home channel
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: • calibration-done – Event calibration done • calibration-started – Event calibration started • channel-change – Event channel change • config-cleared – Configuration cleared event • cov-hole-recovery – Event coverage hole recovery • cov-hole-recovery-done – Event coverage hole recovery done • interference-recovery – Event interference recovery • neighbor-recovery – Event neighbor recovery • power-adjustment – Event power adjustment • root-recovery – Event meshpoint root recovery
smtpnot	Enables and configures logging of the following SMTP module related events: • cfg – Event cfg • cfginc – Event cfg inc • net – Event net • proto – Event proto • smtpauth – Event SMTP authentication • smtperr – Event SMTP error • smtpinfo – Event SMTP information

<event-type>	<event-name>
system	Enables and configures logging of the following system module related events: • clock-reset – Event clock reset • cold-start – Event cold start • config-commit – Event configuration commit • config-revision – Event config-revision done • devup-rfd-fail – Event device-upgrade failed on rf-domain manager managed devices • guest-user-exp – Event guest user purging • http-err – Event Web server did not start • login – Event successful login • login-fail – Event login fail. Occurs when user authentication fails. • login-fail-access – Event login fail access. Occurs in case of access violation. • login-fail-bad-role – Event login fail bad role. Occurs when user uses an invalid role to logon. • 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 password-entry on page 1531. • 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 password-entry on page 1531. • logout – Event logout • maat-light – Event action on RIM *(Research in Motion)* radio(s) from the Maat light module • panic – Event panic • periodic-heart-beat – Event periodic heart beat • procstop – Event proc stop • server-unreachable – Event server-unreachable • system-autoup-disable – Event system autoup disable • system-autoup-enable – Event system autoup enable • t5-config-error – Event t5-config-error • ui-user-auth-fail – Event user authentication fail • ui-user-auth-success – Event user authentication success • warm-start – Event warm start • warm-start-recover – Event recovery from warm start

<event-type>	<event-name>
test	Enables and configures logging of the following test module related events: • testalert – Event test alert • testargs – Event test arguments • testcrit – Event test critical • testdebug – Event test debug • testemerg – Event test emergency • testerr – Event test error • testinfo – Event test information • testnotice – Event test notice • testwarn – Event test warning
tron	Enables and configures logging of the following TRON device (i.e., the ID Nodes) related events: • first-sighting - Logs an event when 'a first-sighting TRON message is generated for the ID node'. • offline - Logs an event when 'an off-line TRON message is generated for the node'. • online - Logs an event when 'an on-line TRON message is generated for the node'. • sporadic - Logs an event when 'a sporadic TRON message is generated for the ID node'.
vrrp	Enables and configures logging of the following *Virtual Router Redundancy Protocol* (VRRP) related events: • vrrp-monitor-change – Event VRRP monitor link state change • vrrp-state-change – Event VRRP state transition • vrrp-vip-subnet-mismatch – Event VRRP IP not overlapping with an interface addresses
webf	Enables and configures logging of the following Web Filtering (webf) module related events: • malform-url-request – Event malformed URL request • no-parent-engine – Event 'no session to URL classification server' • srvr-connect-fail – Event URL classification server unreachable • url-blocked – Event URL blocked • webf-lic-acquired – Event webf license acquired • webf-lic-missing – Event webf license missing • webf-lic-revoked – Event webf license revoked

<event-type>	<event-name>
wips	Enables and configures logging of the following Wireless IPS module related events: • air-termination-active – Event air termination active air-termination-ended – Event air termination ended air-termination-inactive – Event air termination inactive air-termination-initiated – Event air termination initiated rogue-ap-active – Event rogue AP active rogue-ap-inactive – Event rogue AP inactive unsanctioned-ap-active – Event unsanctioned AP active unsanctioned-ap-inactive – Event unsanctioned AP inactive unsanctioned-ap-status-change – Event unsanctioned AP changed state wips-client-blacklisted – Event WIPS client blacklisted • wips-client-rem-blacklist – Event WIPS client rem blacklist • wips-event – Event WIPS event triggered Note: Air-termination is not supported on AP505 and AP510 model access points.
email	Sends e-mail notifications to a pre configured e-mail ID
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 (event-system-policy-config-mode) on page 366	Resets or disables event monitoring

no (event-system-policy-config-mode)

Negates an event monitoring configuration

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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

event on page 352	Configures the action taken for each event

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing firewall policy

Note
For more information on Firewall policy, see Firewall Policy on page 1481.

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 *Access Control List* (ACL). 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 use (profile/device-config-mode-commands) on page 1247. 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 association-list on page 529.

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-testAP505)#use global-association-list server vtt-list
rfs4000-880DA7(config-profile-testAP505)#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-testAP505)#
```

On the access point's device context:

```
ap505-13403B(config-device-94-9B-2C-13-40-38)#use global-association-list server vtt-
list
ap505-13403B(config-device-94-9B-2C-13-40-38)#show context include-factory | in
clude global-association-list
 use global-association-list server vtt-list
ap505-13403B(config-device-94-9B-2C-13-40-38)#
```

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
rfs4000-880DA7(config-device-00-23-68-88-0D-A7)#
```

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 NX9500 and NX7500 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 NX9500 and NX7500 model service platforms respectively.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing guest management policy

guest-management-policy config commands

The following table summarizes guest management policy configuration mode commands:

Table 18: Guest Management Policy Config Commands

Command	Description
email on page 371	Configures guest user e-mail notification settings
guest-database-backup on page 373	Enables periodic backup of the captive portal's guest registration user database
guest-database-export on page 374	Schedules an export of the Guest Management User database to a specified external server
sms on page 375	Configures guest user SMS notification settings
sms-over-smtp on page 377	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.
no (guest-management-policy-config-commands) on page 379	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 75XX, NX 95XX, NX 96XX, VX 9000

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/HOSTNAME>| <HOST-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. • <IP/HOSTNAME> – Specify the SMTP server's IPv4 address or hostname. • <HOST-ALIAS-NAME> – 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.
sender <EMAIL-ADDRESS>	Configures the sender's name for the guest user receiving the passcode required for registering their guest E-mail credentials using SMTP. • <EMAIL-SENDER> – Specify the sender's name (should not exceed 100 characters).
security [none|ssl|starttls]	Configures the encryption protocol used by the SMTP server when communicating the pass code • none – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination. • SSL – Uses SSL encryption. This is the default setting. • STARTTLS – Uses STARTTLS encryption
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. • <USER-NAME> – Specify the username (should not exceed 100 characters).
password <PASSWORD>	Configures the password associated with the specified SMTP user name • <PASSWORD> – Specify the password (should not exceed 63 characters).

```
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) • <LINE> – Specify the message content. When entering the message, use the following tags: GM-NAME – for the guest user's name GM_PASSCODE – for the pass code CR-NL – to enter a new line For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this for internet access.

```
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) • <LINE> – Specify the subject line content. When entering the subject line, use the following tag: GM-NAME – for the guest user's name For example: GM_NAME, your internet access code

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 (guest-management-policy-config-commands) on page 379	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 75XX, NX 95XX, NX 96XX, VX 9000

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). • <TIME> – 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.

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

no (guest-management-policy-config-commands) on page 379	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 75XX, NX 95XX, NX 96XX, VX 9000

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 • <TIME> – Configures the start time of the export operation in the HH:MM format
frequency <1-168>	Configures the user collection export frequency in hours • <1-168> – 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.
url-directory <URL>	Configures external server's URL and directory to where the collection is exported • <URL> – Specify the external server's URL

format [csv|json]	Optional. Configures the file format • csv – Exports collection to the specified location in CSV format. This is the default setting. • json – Exports collection to the specified location in JSON format
last-visit-within <1-168>	Configures a filters guest users who have last visited within a specified period of time • <1-168> – 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.

Examples

```
nx9500-6C8809(config-guest-management-gm1)#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 (guest-management-policy-config-commands) on page 379	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 75XX, NX 95XX, NX 96XX, VX 9000

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. • <USER-NAME> – Specify the username (should not exceed 32 characters).
password <PASSWORD>	Configures the password associated with the specified username • <PASSWORD> – Specify the password (should not exceed 63 characters).
api-id <ID>	Set a 32 character maximum API ID • <API-ID> – Specify the API ID (should not exceed 32 characters).
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 • <WORD> – Specify the source number (should not exceed 32 characters).

```
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) • <LINE> – Specify the message content. When entering the message, use the following tags: GM-NAME – for the guest user's name GM_PASSCODE – for the pass code For example: Dear GM_NAME, your internet access pass code is GM_PASSCODE.

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 (guest-management-policy-config-commands) on page 379	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 75XX, NX 95XX, NX 96XX, VX 9000

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. • <IP/HOSTNAME> – Specify the SMTP gateway server resource's IP address or hostname. • <HOST-ALIAS-NAME> – 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.
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. • <EMAIL-ADDRESS> – Specify the e-mail address (should not exceed 64 characters).
security [none|ssl|starttls]	Configures the encryption protocol used by the SMTP server when communicating the pass code • none – No encryption used. Use if no additional user authentication is needed beyond the required username and password combination. • SSL – Uses SSL encryption. This is the default setting. • STARTTLS – Uses STARTTLS encryption
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. • <USER-NAME> – Specify the username (should not exceed 64 characters).
password <PASSWORD>	Configures the password associated with the specified SMTP user name • <PASSWORD> – Specify the password (should not exceed 64 characters).
recipient <EMAIL-ADDRESS>	Configures the e-mail recipient's e-mail address • <EMAIL-ADDRESS> – Specify the recipient's e-mail address (should not exceed 64 characters in length.

```
sms-over-smtp message <LINE>
```

sms-over-smtp	Configures guest user SMS over SMTP notification message content
message <LINE>	Configures the content of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 1024 characters) • <LINE> – Specify the message content. When entering the message, use the following tags: GM-NAME – for the guest user's name GM_PASSCODE – for the pass code CR-NL – to enter a new line For example: Dear GM_NAME, CR-NL your internet access pass code is GM_PASSCODE. CR-NL Use this access code for internet access.

```
sms-over-smtp subject <LINE>
```

sms-over-smtp	Configures guest user e-mail notification subject line content
subject <LINE>	Configures the subject line of the SMS over SMTP sent to the guest user notifying the pass code (should not exceed 100 characters) • <LINE> – Specify the subject line content. When entering the subject line, use the following tag: GM-NAME – for the guest user's name For example: GM_NAME, your internet access code

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

no (guest-management-policy-config-commands) on page 379	Removes the SMS over SMTP settings used to send SMS to the guest user

no (guest-management-policy-config-commands)

Removes this guest management policy settings

Supported in the following platforms:

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

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
vnx9500-6C8809(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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Disables storing of the encryption key in the startup configuration file
password-encryption on page 427	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
  server        ESL server
  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

no on page 611	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 19: IoT-Device-Type Imagotag Policy Config Commands

Command	Description
channel (iot-device-type-imagotag-policy) on page 383	Configures the channel assigned for ESL communicator to tag communication in the 2.4 GHz band
enable (iot-device-type-imagotag-policy) on page 384	Enables the ESL communicator
fcc-mode (iot-device-type-imagotag-policy) on page 384	Enables the FCC compatibility mode on the ESL communicator
output-power (iot-device-type-imagotag-policy) on page 385	Configures the maximum output power for the ESL communicator
payload-size (iot-device-type-imagotag-policy) on page 386	Configures the maximum payload size in packets exchanged between ESL communicator and tags
server (iot-device-type-imagotag-policy) on page 387	Configures the ESL SES-Imagotag server's hostname or IP address
ssl (iot-device-type-imagotag-policy) on page 388	Enables SSL *(Secure Socket Layer)* encryption mode of communication between the AP and the SES-imagotag server.
window-size (iot-device-type-imagotag-policy) on page 387	Configures the transmission window size for messages exchanged between ESL communicator and tags.
no (iot-device-type-imagotag-policy) on page 389	Reverts this IoT Device-Type Imagotag policy settings to default values

channel (iot-device-type-imagotag-policy)

Manually configures the channel assigned for the *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]	Configures the 2.4 GHz frequency channel, using one of the following options: • <0-10> – Manually configures the channel from 0 - 10. • acs – Enables ACS channel selection mode. This is the default setting.

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

no (iot-device-type-imagotag-policy) on page 389	Reverts the channel selection mode to ACS

enable (iot-device-type-imagotag-policy)

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

no (iot-device-type-imagotag-policy) on page 389	Disables the ESL communicator

fcc-mode (iot-device-type-imagotag-policy)

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

no (iot-device-type-imagotag-policy) on page 389	Disables FCC compatibility mode

output-power (iot-device-type-imagotag-policy)

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]
```

output-power [Level-A|Level-B|Level-C|Level-D|Level-E|Level-F|Level-G|Level-H]	Configure the ESL communicator's output power in dBm. The options are: • Level-A – 1 dBm. This is the default setting. • Level-B - -4 dBm • Level-C - -6 dBm • Level-D - -12 dBm • Level-E - 0 dBm • Level-F - -2 dBm • Level-G - -8 dBm • Level-H - -10 dBm Note: SES-Imagotags recommends NOT to change the default setting, which is in conformance to various country/region specific RF regulations.

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

no (iot-device-type-imagotag-policy) on page 389	Reverts the ESL communicator's output-power to default (Level-A)

payload-size (iot-device-type-imagotag-policy)

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 (iot-device-type-imagotag-policy) on page 389	Reverts the payload size to default (32 bytes)

window-size (iot-device-type-imagotag-policy)

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 (iot-device-type-imagotag-policy) on page 389	Reverts the window-size to 14 bytes.

server (iot-device-type-imagotag-policy)

Configures the ESL SES-Imagotag server's IP address or hostname. As per the current implementation, at the ESL server end, the WiNG AP's IP address was configured to enable the server contact the AP and establish connection with the ESL communicator (USB Dongle). Starting with WiNG 5.9.3, the WiNG AP will send a connection request to the ESL server. For this purpose, the ESL Imagotag server's IP address or hostname has to be configured in the IOT Imagotag policy. Use this command to provide the SES-Imagotag server's IP address or hostname.

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

```
server [hostname|ip-address]
server [hostname <HOST-NAME>|ip-address [<IP>|<HOST-ALIAS-NAME>]] {port <1-65535>}
```

Parameters

```
server [hostname <HOST-NAME>|ip-address [<IP>|<HOST-ALIAS-NAME>]] {port <1-65535>}
```

server	Configures the ESL server's hostname or IP address
hostname <HOST-NAME>	Use this option to configure the ESL server's hostname. • <HOSTNAME> – Provide the hostname (could be FQDN, partial DN, etc.)
ip-address [<IP>|<HOST-ALIAS-NAME>]	Use this option to configure the ESL server's IP address • <IP> – Provide the IP address • <HOST-ALIAS-NAME> – Provide a host alias name. Note, if using this option, ensure that the host alias is existing and pointing to the ESL server host.
port <1-65535>	Optional. Configures the port on which the ESL server can be reached. • <1-65535> – Specify the port from 1 - 65535.

Examples

```
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#server ip-address
10.234.160.225
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#show context
 iot-device-type-imagotag-policy test
  enable
  output-power Level-B
  window-size 12
  payload-size 25
  ssl
  fcc-mode
  channel 9
  server ip-address 10.234.160.225
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#
```

Related Commands

no (iot-device-type-imagotag-policy) on page 389	Removes the ESL server's hostname or IP address configuration

ssl (iot-device-type-imagotag-policy)

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 (iot-device-type-imagotag-policy) on page 389	Disables SSL encryption mode of communication

no (iot-device-type-imagotag-policy)

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|server|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:

```
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#no ?
iot-device-type-imagotag-policy test
  enable
  output-power Level-B
  window-size 12
  payload-size 25
  ssl
  fcc-mode
  channel 9
  server ip-address 10.234.160.225
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#no payload-size
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#no window-size
NOC-NX9500(config-iot-device-type-imagotag-policy-test)#no server
```

The following example shows the Imagotag policy settings after the 'no' commands are executed:

```
nx9500-6C8809(config-iot-device-type-imagotag-policy-test)#show context
 iot-device-type-imagotag-policy test
  enable
  output-power Level-B
  ssl-enable
  fcc-enable
  channel 9
nx9500-6C8809(config-iot-device-type-imagotag-policy-test)#
```

ip

Creates an *access control list* (ACL) and enters its configuration mode. 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Creates an EX3500 Extended ACL and enters its configuration mode • <EX3500-EXT-ACL-NAME> – Specify the ACL name. If an ACL with the specified name does not exist, it is created.

```
ip ex3500-std-access-list <EX3500-STD-ACL-NAME>
```

ex3500-std-access-list <EX3500-STD-ACL-NAME>	Creates an EX3500 Standard ACL and enters its configuration mode • <EX3500-EXT-ACL-NAME> – Specify the ACL name. If an ACL with the specified name does not exist, it is created.

```
ip snmp-access-list <IP-SNMP-ACL-NAME>
```

snmp-access-list <IP-SNMP-ACL-NAME>	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. Use SNMP ACLs (firewalls) to help reduce SNMP's vulnerabilities, as SNMP traffic can be easily exploited to produce a DoS. • <IP-SNMP-ACL-NAME> – 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. To link the SNMP community string with the SNMP IP ACL, in the management-policy-config-mode, use the following command: `snmp-server > community <COMMUNITY-STRING> > [ro|rw] > ip-snmp-access-list <IP-SNMP-ACL-NAME>`.

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

no on page 611	Removes an existing IP access control list

Note
For more information on Access Control Lists, see Access-List Policy on page 1353.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ipv6 access-list <IPv6-ACL-NAME>
```

Parameters

```
ipv6 access-list <IPv6-ACL-NAME>
```

access-list <IPv6-ACL-NAME>	Configures an IPv6 access list and enters its configuration mode • <IPv6-ACL-NAME> – Specify the IPv6 ACL name. If the access list does not exist, it is created.

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

no on page 611	Removes an IPv6 access control list

Note
For more information on access control lists, see Access-List Policy on page 1353.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
rfs4000-229D58NOC-NX9500(config)#ipv6-router-advertisement-policy test
rfs4000-229D58NOC-NX9500(config-ipv6-radv-policy-test)#?
IPv6 Router Advertisement Policy Mode commands:
  advertise                       Option to advertise in router advertisement
  assist-neighbor-discovery       Send the Source Link Layer address option
                                  in Router Advertisement to assist in
                                  neighbor discovery
  check-ra-consistency            Check if the parameters advertised by other
                                  routers on the link are in conflict with
                                  those configured on this router. Conflicts
                                  are logged.
  dns-server                      DNS Server
  domain-name                     Configure domain-name
  managed-config-flag             Set the managed-address-configuration flag
                                  in Router Advertisements. When set, it
                                  indicates that the addresses are available
                                  via DHCPv6
```

```
  nd-reachable-time                 Time that a node assumes a neighbor is
                                    reachable after having received a
                                    reachability confirmation
  no                                Negate a command or set its defaults
  ns-interval                       Time between retransmitted Neighbor
                                    Solicitation messages
  other-config-flag                 Set the other-configuration flag in Router
                                    Advertisememts. When set, it indicates that
                                    other configuration information is
                                    available via DHCPv6.
  ra                                Router Advertisements
  router-lifetime                   Lifetime associated with the default router
  router-preference                 Preference of this router over other
                                    routers
  unicast-solicited-advertisement   Unicast the solicited Router Advertisements

  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-radv-policy-test)#
```

Related Commands

no on page 611	Removes the specified IPv6 RA policy

ipv6-router-advertisement-policy config commands

The following table summarizes the IPv6 *router advertisement* (RA) policy configuration mode commands:

Table 20: IPv6 Router Advertisement Policy Config Commands

Command	Description
advertise on page 395	Enables advertisement of IPv6 MTU *(maximum transmission unit)* and hop-count value in RAs
assist-neighbor-discovery on page 395	Enables advertisement of the source link layer address in RAs
check-ra-consistency on page 396	Enables checking of consistency in RA values advertised by this router with those advertised by other routers, if any, on the same link
dns-server on page 396	Configures the DNS server's IPv6 address and lifetime advertised in RAs
domain-name on page 397	Configures the Domain name search label advertised in RAs
managed-config-flag on page 398	Sets the managed address configuration flag in RAs
nd-reachable-time on page 399	Enables advertisement of neighbor reachable time in RAs
ns-interval on page 400	Configures the interval between two successive retransmitted NS *(neighbor solicitation)* messages

Table 20: IPv6 Router Advertisement Policy Config Commands (continued)

Command	Description
other-config-flag on page 400	Sets the other-configuration flag in RAs
ra on page 401	Configures RA related parameters, such as the interval between two unsolicited successive RAs
router-lifetime on page 402	Configures the default router's lifetime, in seconds, advertised in RAs
router-preference on page 402	Configures the router preference field value advertised in RAs
unicast-solicited-advertisement on page 403	Enables unicasting of solicited RAs
no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
advertise [hop-limit|mtu]
```

Parameters

```
advertise [hop-limit|mtu]
```

advertise [hop-limit|mtu]	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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
assist-neighbor-discovery
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#assist-neighbor-discovery
```

Related Commands

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}
```

Parameters


```
dns-server <IPv6> {lifetime [<4-3600>|expired|infinite]}
```


dns-server <IPv6>	Configures the DNS server's IPv6 address 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. • <IPv6> – Specify the DNS server's address. This address is advertised in RAs. A maximum of four (4) entries can be made per policy.
lifetime [<4-3600>|expired|infinite]	Optional. Configures the DNS server's (identified by the <IPv6> parameter) lifetime • <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds. • expired – Advertises that this DNS server's lifetime has expired and should not be used • infinite – Advertises that this DNS server's lifetime is infinite

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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. • <WORD> – Specify the Domain name search label. A maximum of four (4) entries can be made per policy.
lifetime [<4-3600>| expired|infinite]	Optional. Configures the Domain name search label's lifetime • <4-3600> – Configures a lifetime in seconds. Specify a value form 4 - 3600 seconds. The default is 600 seconds. • expired – Advertises that this Domain name search label's lifetime has expired and should not be used • infinite – Advertises that this Domain name search label's lifetime is infinite

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (ipv6-ra-policy-config-commands) on page 404	Removes the managed address configuration flag advertised in RAs

nd-reachable-time

Enables advertisement of *neighbor discovery* (ND) reachable time in RAs. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
nd-reachable-time [<5000-3600000>|global]
```

Parameters

```
nd-reachable-time [<5000-3600000>|global]
```

nd-reachable-time [<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: • <5000-3600000> – Configures an interface-specific value. Specify a value from 5000 - 3600000 milliseconds. The default is 5000 milliseconds. • global – Advertises the neighbor reachable time configured for the system. This is the value configured at the device configuration mode. For more information, see use (profile/device-config-mode-commands) on page 1247 (profile config mode).

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <1000-3600000> – Specify a value from 1000 - 3600000 milliseconds. The default is 1000 milliseconds. • global – Advertises the NS interval configured for the system. This is configured on the device in the device configuration mode. For more information, see ipv6 on page 1175 (profile config mode).

Examples

```
nx9500-6C8809nx9500-6C8809(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

no (ipv6-ra-policy-config-commands) on page 404	Disables advertisement of NS interval in RAs

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
other-config-flag
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-ipv6-radv-policy-test)#other-config-flag
```

Related Commands

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <3-1800> – Specify a value from 3 - 1800 seconds. The default is 300 seconds. Note: The router-lifetime should be at least three times the specified router interval.
suppress	Enables the suppression of RAs. When enabled, the transmission of RAs in IPv6 packets is suppressed. This option is disabled by default. The `no > ra > suppress` 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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
router-lifetime <0-9000>
```

Parameters

```
router-lifetime <0-9000>
```

router-lifetime <0-9000>	Configures the default router's lifetime • <0-9000> – Specify a value from 0 - 9000 seconds. The default value is 1500 seconds. **Note:** A value of "0" indicates that this router is not the default router.

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
router-preference [high|medium|low]
```

Parameters

```
router-preference [high|medium|low]
```

router-preference [high|medium|low]	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: • For a router to be selected as a default router, the router's lifetime should not be equal to "0". • To enable default router selection, using router information contained in RAs, configure default router selection on that interface.

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

no (ipv6-ra-policy-config-commands) on page 404	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (ipv6-ra-policy-config-commands) on page 404	Disables unicasting of solicited RAs

no (ipv6-ra-policy-config-commands)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

no <PARAMETERS>	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 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

Parameters

```
l2tpv3 policy <L2TPV3-POLICY-NAME>
```

l2tpv3 policy <L2TPV3-POLICY-NAME>	Configures an L2TPV3 tunnel policy • <L2TPV3-POLICY-NAME> – Specify a policy name. If a policy with the specified does not already exist, it is created. To modify an existing L2TPV3, specify its name.

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

no on page 611	Removes an existing L2TPV3 tunnel policy
mint-policy on page 414	Configures the global MiNT policy

Note
For more information on the L2TPV3 tunnel configuration mode and commands, see l2tpv3 on page 404.

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.

Supported in the following platforms:

- Access Points — AP510, AP505
- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing Location policy from the system

location-policy-config-mode commands

The following table summarizes the Location Policy configuration commands:

Table 21: Location Policy Config Mode Commands

Command	Description
enable on page 407	Enables the location policy
location-key on page 408	Configures the ExtremeLocation Tenant's API key. This key is used by the WiNG controller to authenticate with the ExtremeLocation server.
server-host on page 408	Configures the ExtremeLocation server's hostname
no (location-policy-config-commands) on page 409	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 95XX, 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

no (location-policy-config-commands) on page 409	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-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 95XX, VX 9000

Syntax

```
location-key <API-KEY>
```

Parameters

```
location-key <API-KEY>
```

location-key <API-KEY>	Enter the 64-bit key that the WiNG controller uses to authenticate with the ExtremeLocation server. • <API-KEY> – Enter the key. Note: To generate API-Key, log into your ExtremeLocation Tenant account and use the ExtremeLocation UI. Enter that key here in the Location Policy.

Examples

```
nx9500-6C8809(config-location-policy-ELocPolicy)#location-key dGVzdEAxMjM0NQo
vnx9500-6C8809(config-location-policy-ELocPolicy)#show context
location-policy ELocPolicy
 enable
 location-key dGVzdEAxMjM0NQo
nx9500-6C8809(config-location-policy-ELocPolicy)#
```

Related Commands

no (location-policy-config-commands) on page 409	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 95XX, VX 9000

Syntax

```
server-host 1 ip <HOSTNAME> {port <1-65535>}
```

Parameters

```
server-host 1 ip <HOSTNAME> {port <1-65535>}
```

server-host 1 ip <HOSTNAME>	Identifies the ExtremeLocation server by its hostname • <HOSTNAME> – Enter ExtremeLocation server's hostname. **Note:** 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.
{port <1-65535>}	optional. Configures the port on which the ExtremeLocation server is reachable • <1-63335> – Selects a port from 1 - 65535 for the ExtremeLocation server. **Note:** By default the ExtremeLocation server is reachable on port 443.

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 (location-policy-config-commands) on page 409	Removes ExtremeLocation server's hostname from the policy

no (location-policy-config-commands)

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 95XX, 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 paremeters 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 dGVzdEAxMjM0NQo
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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mac access-list <MAC-ACL-NAME>
```

Parameters

```
mac access-list <MAC-ACL-NAME>
```

access-list <MAC-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

no on page 611	Removes an existing MAC access control list

Note
For more information on Access Control Lists, seeAccess-List Policy on page 1353 .

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
management-policy <MANAGEMENT-POLICY-NAME>
```

Parameters

```
management-policy <MANAGEMENT-POLICY-NAME>
```

<MANAGEMENT-POLICY-NAME>	Specify the management policy name. If a policy with the specified name 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 on page 611	Removes an existing management policy

Note
For more information on Management policy configuration, see Management Policy on page 1518.

meshpoint

Creates a new meshpoint and enters its configuration mode. Use this command to select and configure existing meshpoints.

Note
The WiNG 7.1.X release does not support Meshpoint configuration on AP5XX model access points. This feature will be supported in future releases.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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

no on page 611	Removes an existing meshpoint

Note
For more information on Meshpoint configuration, see Meshpoint Policy on page 1773.

meshpoint-qos-policy

Configures a set of parameters that defines the meshpoint QoS policy.

Note
The WiNG 7.1.X release does not support Meshpoint configuration on AP5XX model access points. This feature will be supported in future releases.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 on page 611	Removes an existing meshpoint QoS policy

Note
For more information on Meshpoint QoS policy configuration, see Meshpoint Policy on page 1773.

mint-policy

Configures the global MiNT policy and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1512.

nac-list

Configures a *Network Access Control* (NAC) 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing NAC list

nac-list-mode-commands

The following table summarizes NAC list configuration mode commands:

Table 22: NAC-List Config Mode Commands

Command	Description
exclude on page 416	Specifies the MAC addresses excluded from the NAC enforcement list
include on page 417	Specifies the MAC addresses included in the NAC enforcement list
no (nac-list-config-commands) on page 418	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <START-MAC> – Specify the first MAC address in the range. Note: Use this parameter to specify a single MAC address.
<END-MAC>	Specifies the last MAC address in the range (optional if a single MAC is added to the list) • <END-MAC> – Specify the last MAC address in the range.
precedence <1-1000>	Sets the rule precedence. Exclude entries are checked in the order of their rule precedence. • <1-1000> – Specify a value from 1 - 1000.

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

no (nac-list-config-commands) on page 418	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <START-MAC> – Specify the first MAC address in the range. Note: Use this parameter to specify a single MAC address.
<END-MAC>	Specifies the last MAC address in the range (optional if a single MAC is added to the list) • <END-MAC> – Specify the last MAC address in the range.
precedence <1-1000>	Sets the rule precedence. Include entries are checked in the order of their rule precedence. • <1-1000> – Specify a value from 1 - 1000.

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 (nac-list-config-commands) on page 418	Removes an include rule from this NAC list

no (nac-list-config-commands)

Cancels an exclude or include NAC list rule

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

nsight-policy (global-config-mode)

Creates an NSight policy and enters its configuration mode. Starting with WiNG 5.9.4, Extreme NSight is a separate target, with the Extreme NSight server enabled on an external VM appliance. On the WiNG controller, the NSight policy configures this external NSight server's IP address or hostname.

Configure the NSight policy and apply to the RF Domain context. When applied, the RF Domain manager posts statistics (polled from devices within the RF Domain) to the external Extreme NSight server specified in the policy.

Note
Extreme NSight is a licensed feature. For more information on Extreme NSight™, please refer to the Extreme NSight™ User Guide, available at https://extremenetworks.com/documentation.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

Syntax

```
nsight-policy <NSIGHT-POLICY-NAME>
```

Parameters

```
nsight-policy <NSIGHT-POLICY-NAME>
```

<NSIGHT-POLICY-NAME>	Specify the NSight policy name. If a policy with the specified name 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
  mandatory           Configure mandatory app stats reporting
  no                  Negate a command or set its defaults
  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 on page 611	Removes an existing NSight policy

nsight-policy config commands

The following table summarizes NSight policy configuration mode commands:

Table 23: NSight-Policy Config Mode Commands

Command	Description
enable on page 420	Enables this NSight policy
mandatory on page 420	Enables mandatory *Application Visibility and Control* (AVC) statistics reporting
server on page 425	Configures the external NSight server host's IP address or hostname.
no (nsight-policy-config-commands) on page 425	Removes this NSight policy settings

enable

Enables this NSight policy. The default setting is enabled.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

Syntax

```
enable
```

Parameters

```
None
```

Examples

```
nx9510-6C8A5C(config-nsight-policy-test2)#enable
```

Related Commands

no (nsight-policy-config-commands) on page 425	Disables this NSight policy

mandatory

Enables mandatory *Application Visibility Control* (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 on-premise, Extreme NSight server. By default, only the top-ten applications by usage are reported. This option allows you to configure mandatory stats reporting for applications that are not in the top-ten list.

To enable mandatory stats 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.

The RF Domain manager reports only the top-ten applications, by usage, to the Extreme NSight server. However, if you enable mandatory application stats reporting, applications that are not in the top-ten, most-used applications list are 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, most-used applications identified by the system. Thereby totaling the number to ten.

AVC and statistics reporting is available on both the WiNG 5.9.X and WiNG 7.1.X operating systems. However, the DPI engine used to check the data points varies. The WiNG 7.1.2 OS uses *EAA*, formerly

known as Purview™, and WiNG 5.9.X uses a third-party DPI engine. Consequently, the configuration differs depending on AP type. Refer to the following for configuration details required for WiNG 5.9.X and WiNG 7.1.X APs:

- Example 1: Configuring mandatory, app-usage stats reporting for WiNG 5.9.X APs. on page 421
- Example 2: Configuring mandatory, app-usage stats reporting for the new, WiNG 7.1.X, AP5XX APs. on page 422
- Example 3: Configuring mandatory, app-usage stats reporting in a mixed deployment of WiNG 5.9.X and WiNG 7.1.X APs. on page 423

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

Syntax

```
mandatory app stats [app-group|purview-app-group]
mandatory app stats app-group <APP-GROUP-NAME>
mandatory app stats purview-app-group <PURVIEW-APP-GROUP-NAME>
```

Parameters

```
mandatory app stats app-group <APP-GROUP-NAME>
```

mandatory app stats	Enables mandatory, app-usage stats reporting for a specified *application group*
app-group <APP-GROUP-NAME>	Specifies the application group for which usage statistics reporting is to be made mandatory. Use this option for the WiNG 5.9.X access points that use a third-party DPI engine for data inspection. • <APP-GROUP-NAME> – Specify the application group name.

```
mandatory app stats purview-app-group <PURVIEW-APP-GROUP-NAME>
```

mandatory app stats	Enables mandatory, app-usage stats reporting for a specified *purview application group*
app-group <PURVIEW-APP-GROUP-NAME>	Specifies the Purview application group for which usage statistics reporting is to be made mandatory. Use this option for the new, 802.11ax, WiNG 7.1.X access points that use the Purview™ DPI engine for data inspection. • <PURVIEW-APP-GROUP-NAME> – Specify the Purview application group name.

Example 1: Configuring mandatory, app-usage stats reporting for WiNG 5.9.X APs.

The WiNG 5.9.X APs use a third-party DPI engine. If you have WiNG 5.9.X APs adopted to a WiNG 7.1.X controller, follow the steps below to enable mandatory, app-usage stats reporting:

1 Create an application-group.

```
<CONTROLER>(config)#application-group <APP-GROUP-NAME>
```

Example,

```
nx9500-6C8809(config)#application-group APPGRP
```

a Specify the target applications for which mandatory stats reporting is to be enabled.

```
<CONTROLLER>(config-app-group-APPGRP)#application <APPLICATION-NAME>
```

Example,

```
nx9500-6C8809(config-app-group-APPGRP)#show context
application-group APPGRP
 application ChatCube
 application ChatCube_apache
nx9500-6C8809(config-app-group-APPGRP)#
```

2 Create an NSight policy.

```
<CONTROLER>(config)#nsight-policy <POLICY-NAME>
```

Example,

```
nx9500-6C8809(config)#nsight-policy APPGRP
```

a Enable mandatory stats reporting for the application-group created in Step 1.

```
nx9500-6C8809(config-nsight-policy-APPGRP)#mandatory app stats app-group APPGRP
```

b Specify the NSight server's IP address or hostname.

```
nx9500-6C8809(config-nsight-policy-APPGRP)#server host 1.2.3.4
```

c Enable the NSight policy.

```
nx9500-6C8809(config-nsight-policy-APPGRP)#enable
```

3 Use the NSight policy created in Step 2 in the AP's RF Domain.

For example,

```
nx9500-6C8809(config-rf-domain-APPGRP)#use nsight-policy APPGRP
```

Example 2: Configuring mandatory, app-usage stats reporting for the new, WiNG 7.1.X, AP5XX APs.

The WiNG 7.1.X APs use Extreme Networks' Purview™ DPI engine. Follow the steps below to enable mandatory, app-usage stats reporting on these APs:

1 Create a purview-application-group on page 432.

```
<CONTROLER>(config)#purview-application-group <APP-GROUP-NAME>
```

Example,

```
nx9500-6C8809(config)#purview-application-group PURVIEW
```

a Specify the target applications for mandatory stats reporting.

```
<CONTROLLER>(config-purview-app-group-PURVIEW)#application <APPLICATION-NAME>
```

Example,

```
nx9500-6C8809(config-purview-app-group-PURVIEW)#show context
purview-application-group PURVIEW
 application ChatCube
 application ChatCube_apache
nx9500-6C8809(config-purview-app-group-PURVIEW)#
```

2 Create an NSight policy.

```
<CONTROLER>(config)#nsight-policy <POLICY-NAME>
```

Example,

```
nx9500-6C8809(config)#nsight-policy PURVIEW
```

a Enable mandatory stats reporting for the application-group created in Step 1.

```
nx9500-6C8809(config-nsight-policy-PURVIEW)#mandatory app stats purview-app-group
PURVIEW
```

b Specify the Extreme NSight server's IP address or hostname.

```
nx9500-6C8809(config-nsight-policy-PURVIEW)#server host 1.2.3.4 https
```

c Enable the NSight policy.

```
nx9500-6C8809(config-nsight-policy-PURVIEW)#enable
```

3 Use the NSight policy created in Step 2 in the AP's RF Domain context.

Example,

```
nx9500-6C8809(config-rf-domain-PURVIEW)#use nsight-policy PURVIEW
```

Example 3: Configuring mandatory, app-usage stats reporting in a mixed deployment of WiNG 5.9.X and WiNG 7.1.X APs.

In a mixed deployment, consisting of WiNG 5.9.X and WiNG 7.1.X APs, adopted to a WiNG 7.1.X controller, follow the steps below:

1 Place the WiNG 5.9.X and WiNG 7.1.X APs in separate RF Domains, as shown in the following example.

Example,

```
nx9500-6C8809(config)#show adoption timeline
-------------------------------------------------------------------------------
      AP-NAME    RF-DOMAIN    EVENT      TIME-STAMP        TIME-SINCE-EVENT
-------------------------------------------------------------------------------
   ap7562-84A224   WiNG5     adopted   2019-05-08 15:56:30   0 days 01:25:56
   ap7532-DF9A4C   WiNG5     adopted   2019-05-08 15:56:30   0 days 01:25:56
    ap505-134038   WiNG7     adopted   2019-05-08 15:56:30   0 days 01:25:56
   ap8432-070235   WiNG5     adopted   2019-05-08 15:56:28   0 days 01:25:58
-------------------------------------------------------------------------------
Total number of devices displayed: 4
nx9500-6C8809(config)#
```

Note

The WiNG 5.9.X and WiNG 7.1.X APs are placed in the WiNG5 and WiNG7 RF Domains respectively.

2 Create application groups for the WiNG 5.9.X and WiNG 7.1.X APs.

- For the WiNG 5.9.X APs, use the application-group command.

```
<CONTROLER>(config)#application-group <APP-GROUP-NAME>
```

Specify the applications for which mandatory, app-usage stats is to be enabled.

```
<CONTROLLER>(config-purview-app-group-PURVIEW)#application <APPLICATION-NAME>
```

Example,

```
nx9500-6C8809(config-purview-app-group-WiNG5)#show context
application-group WiNG5
 application ChatCube
 application ChatCube_apache
nx9500-6C8809(config-purview-app-group-WiNG5)#
```

- For WiNG 7.1.X APs, use the purview-application-group on page 432 command.

```
<CONTROLER>(config)#purview-application-group <APP-GROUP-NAME>
```

Specify the applications for which mandatory, app-usage stats is to be enabled.

```
<CONTROLLER>(config-purview-app-group-WiNG7)#application <APPLICATION-NAME>
```

Example,

```
nx9500-6C8809(config-purview-app-group-WiNG7)#show context
purview-application-group WiNG7
 application ChatCube
 application ChatCube_apache
nx9500-6C8809(config-purview-app-group-WiNG7)#
```

3 Create two NSight policies and enable mandatory, app-usage stats reporting for the application groups created in Step 1.

- For the WiNG 5.9.X APs:

  Example,

  ```
  nx9500-6C8809(config)#nsight-policy WiNG5
  ```

  1 Enable mandatory stats reporting.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG5)#mandatory app stats app-group WiNG5
  ```

  2 Specify the Extreme NSight server's IP address or hostname.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG5)#server host 1.2.3.4 https
  ```

  3 Enable the NSight policy.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG5)#enable
  ```

- For the WiNG 7.1.X APs:

  Example,

  ```
  nx9500-6C8809(config)#nsight-policy WiNG7
  ```

  1 Enable mandatory stats reporting.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG7)#mandatory app stats purview-app-group
  WiNG7
  ```

  2 Specify the NSight server's IP address or hostname.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG7)#server host 1.2.3.4 https
  ```

  3 Enable the NSight policy.

  ```
  nx9500-6C8809(config-nsight-policy-WiNG7)#enable
  ```

4 Use the appropriate NSight policy in the WiNG 5.9.X and WiNG 7.1.X AP's RF Domains.

- For the WiNG 5.9.X APs:

  ```
  nx9500-6C8809(config-rf-domain-WiNG5)#use nsight-policy WiNG5
  ```

- For the WiNG 7.1.X APs:

  ```
  nx9500-6C8809(config-rf-domain-WiNG7)#use nsight-policy WiNG7
  ```

Related Commands

no (nsight-policy-config-commands) on page 425	Disables mandatory app-usage statistics reporting

server

Configures the external NSight server's IP address or hostname

Note
Starting with WiNG 5.9.4 NSight server cannot be configured on the VX9000, NX9500, or NX9600 platforms. Extreme NSight is a separate target that can only be deployed on an external VM appliance.

Note
For more information on Extreme NSight™, please refer to the Extreme NSight™ User Guide, available at https://extremenetworks.com/documentation.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX900

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's IP address or hostname. Use one of the following options to identify the NSight server: • <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 Note: When this NSight policy is applied to an RF Domain, the RF Domain manager posts statistics (polled from devices within the RF Domain) to the external Extreme NSight server host specified here.
{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
nx9510-6C8A5C(config-nsight-policy-test2)#
```

Related Commands

no (nsight-policy-config-commands) on page 425	Removes NSight server's IP address or hostname configuration from this NSight policy

no (nsight-policy-config-commands)

Removes NSight policy settings or reverts them to default values

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600, VX9000

Syntax

```
no [enable|mandatory app stats app-group <APPLICATION-GROUP-NAME>|server host [<IPv4>|
<HOST-NAME>|<IPv6>]]]
```

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
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:

```
nx9510-6C8A5C(config-nsight-policy-test2)#show context
nsight-policy test2
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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
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 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 passopint 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

rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no on page 611	Removes an existing passpoint policy

Note
For more information on Passpoint policy, see Passpoint Policy on page 1817.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
password-encryption secret 2 <LINE>
```

Parameters

```
password-encryption secret 2 <LINE>
```

secret 2 <LINE>	Encrypts passwords with a secret phrase • 2 – Specifies the encryption type as either SHA256-AES256 • <LINE> – Specify the encryption passphrase.

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 on page 611	Disables password encryption

profile

Configures profile related commands. If no parameters are given, all profiles are selected.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
profile {anyap|ap505|ap510|containing|filter|nx5500|nx75xx|nx9000|nx9600|vx9000}
profile {anyap|ap505|ap510|nx5500|nx75xx|nx9000|nx9600|vx9000} <DEVICE-PROFILE-NAME>
profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap505|ap510||nx75xx|nx9000|
nx9600|
vx9000]}
profile {filter type [ap505|ap510|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000]}
```

Parameters

```
profile {anyap|ap505|ap510|rfs6000|nx5500|nx75xx|nx9000|nx9600|vx9000}
<DEVICE-PROFILE-NAME>
```

profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>	Configures device profile commands. If no device profile is specified, the system configures all device profiles. • <DEVICE-TYPE> – Optional. Select the device type. The options are: AP505, AP510, NX5500, NX7500, NX9500, NX9600, and VX9000. After specifying the device type, specify the profile name. • <DEVICE-PROFILE-NAME> – Specify the profile name. Select 'anyap' to configure a profile applicable to any access point.

```
profile {containing <DEVICE-PROFILE-NAME>} {filter type [ap505|ap510|nx5500|nx75xx|
nx9000|nx9600|vx9000]}
```

profile	Configures device profile commands
containing <DEVICE-PROFILE-NAME>	Optional. Configures profiles that contain a specified sub-string in the hostname • <DEVICE-PROFILE-NAME> – Specify a substring in the profile name to filter profiles.
filter type	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. • type – Filters profiles by the device type. Select a device type from the following options: The options are: AP505, AP510, NX5500, NX7500, NX9500, NX9600, and VX9000.

```
profile {filter type[ap505|ap510|nx5500|nx75xx|nx9000|nx9600|vx9000]}
```

profile	Configures device profile commands
filter type	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. • type – Filters profiles by the device type. Select a device type from the following options: The options are: AP505, AP510, NX5500, NX7500, NX9500, NX9600, and VX9000.

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 Poicy 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

no on page 611	Removes a profile and its associated configurations

Note
For more information on profiles and how to configure profiles, see Profiles on page 848.

purview-application-group

Global Configuration Commands on page 163

Creates a Purview Application Group and enters its configuration mode. A Purview application group is a collection of system-provided and/or user-defined applications. Application group allows you to enforce mandatory stats reporting for specific traffic types.

The WiNG 7.1.2 OS uses *EAA* (Purview™) DPI engine to implement *Application Visibility and Control* (AVC). It detects top-level hosting applications (layer 7) along with the services these applications host.

Use AVC to implement:

- Packet filtering - allow, deny or mark packets based on rules defined in the Purview application policy.
- Mandatory stats reporting - enable mandatory stats reporting for an application or set of applications defined in the Application group.

The `purview-application-group` command is part of the mandatory stats reporting feature. To enable mandatory stats reporting, follow the steps below:

1 Create a Purview application-group, specify the applications for which mandatory stats reporting is to be enabled.

Note
If the required application definition is not system-provided, use the `application` command to create a custom application signature.

2 Use this Purview application-group in the NSight policy.

3 Apply the NSight policy in the RF Domain context.

Note
For more information and examples, see mandatory on page 420.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Note

Purview DPI engine is not supported on the WiNG 5.9.X devices. This supported will be introduced in future releases. For information on enabling mandatory stats reporting on WiNG 5.9.X devices, see application-group.

Syntax

```
purview-application-group <PURVIEW-APP-GROUP-NAME>
```

Parameters

```
purview-application-group <PURVIEW-APP-GROUP-NAME>
```

purview-application-group <PURVIEW-APP-GROUP-NAME>	Creates a Purview application group and enters its configuration mode • <PURVIEW-APP-GROUP-NAME – Specify the application group name. If a Purview application group with the specified name does not exist, it is created. The name should not exceed 32 characters in length.

Examples

```
nx9500-6C8809(config)#purview-application-group PurvAppGrp
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#?
Purview 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-purview-app-group-PurvAppGrp)#
```

Related Commands

no on page 611 (global-config-mode)	Removes an existing Purview application group
application on page 183	Creates an application definition and enters its configuration mode.
purview-application-policy on page 436	Creates a Purview application policy and enters its configuration mode.
nsight-policy (global-config-mode) on page 418	Creates an NSight policy and enters its configuration mode.

application

purview-application-group on page 432

Adds an application definition to this Purview application group. You can add a system-provided or customized (user-defined) application.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
application <PURVIEW-APP-NAME>
```

Parameters

```
application <PURVIEW-APP-NAME>
```

application <PURVIEW-APP-NAME>	Configures the application to be added to this application group • <PURVIEW-APP-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: The Purview™ DPI engine recognizes 36 app categories with 2406 applications. If the desired application is not available as an option, use the application on page 183 command to add it.

Examples

To view all applications supported by the Purview ™ DPI engine, use [TAB], as shown in the following example:

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application[TAB]
Display all 365 possibilities? (y or n)
163_com                          1Fichier
24x7_Media                       2K_Games
360_Software                     360buy
4chan                            4shared
5Dimes                           8Track
9gag                             A_Feed
AB_Tutor                         Abacast
--More--
nx9500-6C8809(config-purview-app-group-PurvAppGrp
```

Select the desired application from the list displayed, as shown in the following examples:

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application Ali[TAB]
Alibaba      Alibaba_Ads  AliExpress   Alipay
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application Alipay
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application Alibaba
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#application AliExpress
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#show context
application-group PurvAppGrp
 application Alipay
 application Alibaba
```

```
application AliExpress
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
```

Related Commands

no on page 435	Removes a specified application from this application group

description

purview-application-group on page 432

Configures a description for this purview application group

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this purview application group that uniquely differentiates it from other existing application groups • <WORD> – Provide a description not exceeding 80 characters in length.

Examples

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#description "This Purview Application
Group contains Alibaba application."
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#show context
purview-application-group PurvAppGrp
 description “This Purview Application Group contains Alibaba application.”
 application Alipay
 application Alibaba
 application AliExpress
 nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
```

Related Commands

no on page 435	Removes the description configured for this purview application group

no

purview-application-group on page 432

Removes this purview application group’s configurations (application and/or description)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
no [application <PURVIEW-APP-NAME>|description]
```

Parameters

```
no [application <PURVIEW-APP-NAME>|description]
```

no <PARAMETERS>	Removes an application associated with this group, and removes the group's description

Examples

The following example displays the purview-application-group 'PurAppGrp' configuration before the execution of 'no' commands:

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#show context
application-group PurvAppGrp
 description "This Purview Application Group contains Alibaba application."
 application Alipay
 application Alibaba
 application AliExpress
 nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#no application Alipay
nx9500-6C8809(config-app-group-amazon)#no description
```

The following example displays the purview-application-group 'PurAppGrp' configuration after the execution of 'no' commands:

```
nx9500-6C8809(config-purview-app-group-PurvAppGrp)#show context
application-group PurvAppGrp
 application Alibaba
 application AliExpress
 nx9500-6C8809(config-purview-app-group-PurvAppGrp)#
```

purview-application-policy

Global Configuration Commands on page 163

Creates a Purview application policy and enters its configuration mode. Application policies allow you to define rules that dictate how each traffic type is managed on your network. An application policy contains application (Layer 7) rules.

An application rule leverages the AP's *deep packet inspection* (DPI) engine to detect the underlying application to which a frame or flow belongs. The rule then applies access control and quality of service actions to all the traffic associated with the application, not just traffic destined for specific IP addresses or ports. The control actions regulate both access control and traffic engineering (rate limit, marking, and prioritization) for applications and groups.

Once created and configured, apply the application policy at the following levels to enforce application assurance:

- RADIUS *change of authorization* (CoA) – In the device/profile configuration mode, use the `application-policy → radius → <PURVIEW-APP-POLICY-NAME>` command to apply the policy to every user successfully authenticated by the RADIUS server. See purview-application-policy on page 1230 in the profile/device context.
- User role – In the role-policy-user-role configuration mode, use the `use → application-policy <PURVIEW-APP-POLICY-NAME>` command to apply the policy to all users assigned to the role. See use on page 1631 in the user-role policy context.
- WLAN – In the WLAN configuration mode, use the `use → application-policy <PURVIEW-APP-POLICY-NAME>` command to apply the policy to all users accessing the WLAN. See use (wlan-config-mode) on page 575
- Bridge VLAN – In the bridge VLAN configuration mode, use the `use → application-policy <PURVIEW-APP-POLICY-NAME>` command to apply the policy for the traffic corresponding to the bridged VLAN. See use on page 908 in the bridge VLAN context.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Note
Purview DPI engine is not supported on the WiNG 5.9.X devices. This supported will be introduced in future releases. For information on creating WiNG 5.9.X application policy, see `application-policy`.

Syntax

```
purview-application-policy <PURVIEW-APP-POLICY-NAME>
```

Parameters

```
purview-application-policy <PURVIEW-APP-POLICY-NAME>
```

purview-application-policy <PURVIEW-APP-POLICY-NAME>	Specify the Purview 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)#purview-application-policy PurAppPolicy
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#?
Purview Application Policy Mode commands:
  allow              Allow packets
  deny               Deny packets
  description        Purview 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-purview-app-policy-PurAppPolicy)#
```

Related Commands

no on page 611 (global-config-mode)	Removes an existing Purview application policy
application on page 183	Creates an application definition and enters its configuration mode. Use this command to create customized application detection signatures.
purview-application-group on page 432	Creates a Purview Application Group and enters its configuration mode.
nsight-policy (global-config-mode) on page 418	Creates an NSight policy and enters its configuration mode.

allow

purview-application-policy on page 436

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 — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
allow [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

Parameters

```
allow [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

allow	Creates an allow rule and configures the match criteria. The match criteria options are: app-category and application.
app-category [<PURVIEW-APP-CATEGORY-NAME>|all]	Uses application category as the match criteria • <PURVIEW-APP-CATEGORY-NAME> – Specify the application category. • all – Select this option to allow all packets irrespective of the application category.
application <PURVIEW-APP-NAME>	Uses application name as the match criteria • application <PURVIEW-APP-NAME> – Specify the application name. Each packet's application is matched with the application specified here. In case of a match, the system forwards the packet. Note: The Purview™ engine recognizes 36 app-categories with 2406 canned applications. If the application you are looking for is not in this list, use the application on page 183 command to add the application to the list.

schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this allow rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – 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 `purview-application-policy → 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. Note: 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 enforcement-time on page 445.

precedence <1-256>	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.
	Let us consider application *Apple_Streaming* belonging to app-category *streaming*.
	The action required is: Allow Apple_Streaming packets and deny all other applications belonging to app-category streaming.
	The rules can be defined as:
	`#allow application Apple_Streaming precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application Apple_Streaming precedence 2`
	Application policy rules are applied in the increasing order of their precedence value. Once the *deny app-category streaming precedence 1* rule is hit, all streaming packets, including Apple_Streaming, are dropped. Consequently, there are no packets left to apply the subsequent allow rule. The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

Examples

The following example shows how to view all built-in, system provided Purview™ applications:

```
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#allow application[TAB]
Display all 365 possibilities? (y or n)
163_com                          1Fichier
24x7_Media                       2K_Games
360_Software                     360buy
4chan                            4shared
```

```
5Dimes                                  8Track
9gag                                    A_Feed
AB_Tutor                                Abacast
ABC_Ads                                 ABC_News
ABC_Player                              About
--More--
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#
```

The following example shows an allow rule with precedence 1.

```
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#allow application Apple_Streaming
precedence 1
```

The following example shows a Purview application policy 'SocialNet' having an *allow* rule with an associated schedule policy named 'Flickr':

```
nx9500-6C8809(config-purview-app-policy-SocialNet)#allow application flickr schedule
Flickr precedence 1
nx9500-6C8809(config-purview-app-policy-SocialNet)#show context
purview-application-policy SocialNet
 description "This application policy relates to Social Networking sites."
 allow application flickr schedule Flickr precedence 1
nx9500-6C8809(config-purview-app-policy-SocialNet)#
```

The schedule policy 'Flickr' configuration is as follows. As per this policy, the above allow rule will apply to all Flickr packets every Friday between 13:00 and 18:00 hours.

```
nx9500-6C8809(config-schedule-policy-Flickr)#show context
schedule-policy Flickr
 description "Allows Flickr traffic on Fridays."
 time-rule days friday start-time 13:00 end-time 18:00
nx9500-6C8809(config-schedule-policy-Flickr)#
```

Related Commands

no on page 452	Removes this allow rule from the Purview application policy

deny

purview-application-policy on page 436

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 — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases..

Syntax

```
deny [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

Parameters

```
deny [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

deny	Creates a deny rule and configures the match criteria. The match criteria options are: app-category and application.
app-category [<PURVIEW-APP-CATEGORY-NAME>|all]	Uses application category as the match criteria • <PURVIEW-APP-CATEGORY-NAME> – Specify the application category name. • all – Select this option to deny all packets irrespective of the application category.
application <PURVIEW-APP-NAME>	Uses application name as the match criteria • <PURVIEW-APP-NAME> – 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. Note: The Purview™ engine recognizes 36 app-categories with 2406 canned applications. If the application you are looking for is not in this list, use the application on page 183 command to add the application to the list.

schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this deny rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – 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 `purview-application-policy → 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time on page 445.

precedence <1-256>	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.
	Let us consider application *Apple_Streaming* belonging to app-category *streaming*.
	The action required is: Allow Apple_Streaming packets and deny all other applications belonging to app-category streaming.
	The rules can be defined as:
	`#allow application Apple_Streaming precedence 1`
	`#deny app-category streaming precedence 2`
	The following configuration is incorrect:
	`#deny app-category streaming precedence 1`
	`#allow application Apple_Streaming precedence 2`
	Application policy rules are applied in the increasing order of their precedence value. Once the *deny app-category streaming precedence 1* rule is hit, all streaming packets, including Apple_Streaming, are dropped. Consequently, there are no packets left to apply the subsequent allow rule. The mark and rate-limit rules are the only two actions that can be combined for a specific application or application category type.

Examples

The following example shows how to view all built-in, system provided Purview™ app-categories:

```
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#allow app-category[TAB]
ads               all               biz               certs
cloud             cloudcpu          corp              custom
db                education         finance           games
health            location          mail              news
other             p2p               proto             realtimecomms
restrictcontent   search            shopping          social
```

```
sports          storage         streaming       travel
unknown         updates         vpn             webapp
webcontent      webfile         webmeet
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#
```

The following example shows a deny rule with precedence 2.

```
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#deny app-category streaming
precedence 2
```

The following example displays an application policy denying app-category 'social'. The policy is enforceable on weekdays from 9:30 AM to 10 PM.

```
nx9500-6C8809(config-purview-app-policy-DenyS-N)#show context
purview-application-policy DenyS-N
 description "This application policy denies Social Networking sites on weedays."
 enforcement-time days weekdays start-time 09:30 end-time 22:00
 deny app-category social precedence 1
nx9500-6C8809(config-purview-app-policy-DenyS-N)#
```

Related Commands

no on page 452	Removes this deny rule from the Purview application policy

description

purview-application-policy on page 436

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 — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
description <LINE>
```

Parameters

```
description <LINE>
```

description <LINE>	Configures this application policy's description • <LINE> – Specify a brief description not exceeding 80 characters in length.

Examples

```
nx9500-6C8809(config-purview-app-policy-SocialNet)#description "This application policy
relates to Social Networking sites."
nx9500-6C8809(config-purview-app-policy-SocialNet)#show context
purview-application-policy SocialNet
```

```
 description "This application policy relates to Social Networking sites."
nx9500-6C8809(config-purview-app-policy-SocialNet)#
```

Related Commands

no on page 211	Removes this application policy's description

enforcement-time

purview-application-policy on page 436

Configures an enforcement time in days and hours. 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 enforce allow/deny/mark/rate-limit rules at different time periods. If absence of a schedule policy, application policy rules are enforced at the enforcement-time specified within the policy. For more information on configuring a schedule policy, see schedule-policy on page 499.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

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	Enforces this application policy on only on the days specified here • sunday – Enforces the policy only on Sundays • monday – Enforces the policy only on Mondays • tuesday – Enforces the policy only on Tuesdays • wednesday – Enforces the policy only on Wednesdays • thursday – Enforces the policy only on Thursdays • friday – Enforces the policy only on Fridays • saturday – Enforces the policy only on Saturdays • all – Enforces the policy on all days. This is the default setting. • weekends – Enforces the policy only on weekends • weekdays – Enforces the policy only on weekdays In case no enforcement time is specified, the application policy is enforced on all days (i.e., always active). 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').
start-time <HH:MM> end-time <HH:MM>	Optional. Configures this application policy's enforcement period • start-time – Configures the start time. This is the time at which the application policy enforcement begins. • end-time – Configures the end time. This is the time at which the application policy enforcement ends. • <HH:MM> – Specify the start and end time in the HH:MM format.

Examples

```
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#enforcement-time days weekends
start-time 10:30 end-time 20:00
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#show context
purview-application-policy PurAppPolicy
 description "This application policy allows Applie_Streaming packets on weekends."
 enforcement-time days weekends start-time 10:30 end-time 20:00
 allow application Apple_Streaming precedence 1
nx9500-6C8809(config-purview-app-policy-PurAppPolicy)#
```

Related Commands

no on page 452	Removes this application policy's enforcement period

logging

purview-application-policy on page 436

Enables DPI application recognition logging. It also sets the logging level.

DPI analyzes packet and packet content headers to determine the nature of network traffic. When enabled, the Purview™ DPI engine inspects layer 7 traffic 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 — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
logging [level|on]
logging on
logging level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

Parameters

```
logging on
```

logging on	Enables logging of application recognition hits made by the Purview™ 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 Purview™ 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-purview-app-policy-Bing)#logging level critical
nx9500-6C8809(config-purview-app-policy-Bing)#show context
purview-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-purview-app-policy-Bing)#
```

Related Commands

no on page 452	Resets the logging level to default (notifications). And the **no** → **logging** → **on** command disables DPI logging.

mark

purview-application-policy on page 436

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 *type of service* (ToS) 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.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
mark [app-category [<APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
[8021p <0-7>|dscp <0-63>] schedule <SCHEDULE-POLICY-NAME> (precedence <1-256>)
```

Parameters

```
mark [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-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 [<PURVIEW-APP-CATEGORY-NAME>|all]	Uses application category as the match criteria • <PURVIEW-APP-CATEGORY-NAME> – Specify the application category. • all – The system marks all packets.
application <PURVIEW-APP-NAME>	Uses application name as the match criteria • <PURVIEW-APP-NAME> – 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. Note: The Purview™ engine recognizes 36 app-categories with 2406 canned applications. If the application you are looking for is not in this list, use the application on page 183 command to add the application to the list.
8021p <0-7>	Marks packets matching the specified criteria with 802.1p priority value • <0-7> – Specify a value from 0 - 7. 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.

dscp <0-63>	Marks packets matching the specified criteria with DSCP ToS code • <0-63> – Specify a value from 0 - 63. 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.
schedule <SCHEDULE-POLICY-NAME>	Schedules an enforcement time for this mark rule by associating a schedule policy with it. Use this parameter to apply rule-specific enforcement time. • schedule <SCHEDULE-POLICY-NAME> – Associates a schedule policy with this 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 `purview-application-policy → 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time on page 445.
precedence <1-256>	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.

Examples

```
nx9500-6C8809(config-purview-app-policy-Bing)#mark app-category video dscp 9 precedence 4

nx9500-6C8809(config-purview-app-policy-Bing)#mark application facetime dscp 10
precedence 5

nx9500-6C8809(config-purview-app-policy-Bing)#show context
purview-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-purview-app-policy-Bing)#
```

Related Commands

no on page 452	Removes this mark rule from the application policy

rate-limit

purview-application-policy on page 436

Creates a rate-limit rule and configures the match criteria

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
rate-limit [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-
NAME>]
([egress|ingress]) rate <50-1000000> max-burst-size <2-1024> schedule <SCHEDULE-POLICY-
NAME> (precedence <1-256>)
```

Parameters

```
rate-limit [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-
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, a rate-limit is applied to packets that match the configured criteria. These packets could be incoming, outgoing, or both. The match criteria options are: *app-category* and *application*.
app-category [<PURVIEW-APP-CATEGORY-NAME>|all]	Uses application category as the match criteria • <PURVIEW-APP-CATEGORY-NAME> – Specify the application category. • all – The system rate-limits all packets irrespective of the application category.
application <PURVIEW-APP-NAME>	Uses application name as the match criteria • <PURVIEW-APP-NAME> – Specify the application name. Each packet's application is matched with the application specified here. In case of a match, the system rate-limits the packet.
[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. • egress – Rate limits outgoing traffic • ingress – Rate limits incoming traffic 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: • rate – Configures the rate limit, in Kbps, for both incoming and outgoing packets • <50-1000000> – Specify the rate limit from 50 - 1000000 Kbps.

max-burst-size	The following parameters are common to the 'egress' and 'ingress' keywords: • max-burst-size – Configures the maximum burst size, in Kbytes, for both incoming and outgoing packets • <2-1024> – Specify the maximum burst size from 2 - 1024 Kbytes.
schedule <SCHEDULE-POLICY-NAME>	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. • schedule <SCHEDULE-POLICY-NAME> – 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 `purview-application-policy → 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'). • <SCHEDULE-POLICY-NAME> – Specify the policy name (should be existing and configured). After applying a schedule policy, specify a precedence for the rule. 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 enforcement-time on page 445 .
precedence <1-256>	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.

Examples

```
nx9500-6C8809(config-purview-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-purview-app-policy-Bing)#show context
purview-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-purview-app-policy-Bing)#
```

Related Commands

no on page 452	Removes this rate-limit rule from the Purview application policy

no

purview-application-policy on page 436

Removes or resets this Purview application policy's settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

Note
Purview DPI engine is not supported on the WiNG 7.1.2 enabled NX5500, NX7500, NX9500, NX9600 and VX9000 platforms. This support will be introduced in future releases.

Syntax

```
no [allow|deny|description|enforcement-time|logging|mark|rate-limit]
no allow [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
precedence <1-256>
no deny [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-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 [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-NAME>]
precedence <1-256>
no rate-limit [app-category [<PURVIEW-APP-CATEGORY-NAME>|all]|application <PURVIEW-APP-
NAME>] precedence <0-256>
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes or resets this Purview application policy settings based on the parameters passed

Examples

The following example shows the Purview application policy 'Bing' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-purview-app-policy-Bing)#show context
purview-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-purview-app-policy-Bing)#
nx9500-6C8809(config-purview-app-policy-Bing)#no allow app-category business precedence 2
nx9500-6C8809(config-purview-app-policy-Bing)#no deny app-category social\ networking
precedence 3
```

The following example shows the Purview application policy 'Bing' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-purview-app-policy-Bing)#show context
purview-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-purview-app-policy-Bing)#
```

radio-qos-policy

Configures a radio QoS policy

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

Parameters

```
radio-qos-policy <RADIO-QOS-POLICY-NAME>
```

<RADIO-QOS-POLICY-NAME>	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)#
```

Related Commands

no on page 611	Removes an existing Radio QoS policy

Note
For more information on radio qos policy, see Radio-QoS Policy on page 1588.

radius-group

Configures RADIUS user group and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing RADIUS group

Note
For more information on RADIUS user group commands, see RADIUS Policy on page 1557.

radius-server-policy

Creates a RADIUS server policy and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing RADIUS server policy

Note
For more information on RADIUS server policy commands, see RADIUS Policy on page 1557.

radius-user-pool-policy

Configures a RADIUS user pool and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

vnx9500-6C8809(config-radius-user-pool-testRadiusUserPool)#
```

Related Commands

no on page 611	Removes an existing RADIUS user pool policy

Note
For more information on RADIUS user group commands, see RADIUS Policy on page 1557.

rename

Renames and existing TLO

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <TLO-NAME> – Specify the TLO's name. This is the TLO that is to be renamed. • <NEW-TLO-NAME> – Specify the new name for this TLO.

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
nx9500-6C8809nx9500-6C8809(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

clone on page 281	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>| <HOSTNAME>]	Identifies the device to replace by its MAC address or hostname • <MAC-ADDRESS> – Identifies the device to replace by its MAC address. Specify the device's existing MAC address. • <HOSTNAME> – Identifies the device to replace by its hostname. Specify the device's hostname.
<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 ap7161-4BF364 ?
  AA-BB-CC-DD-EE-FF New device MAC address
rfs4000-882A17(config)#replace device ap7161-4BF364 00-15-0F-BB-98-30
```

The following example shows an existing AP 7502 (MAC: DD-AA-BB-88-12-43) configuration staged on a VX 9000 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 radio1
  wlan theMOZART bss 1 primary
 interface radio2
  wlan theMOZART bss 1 primary
 interface ge1
  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 AP 7502 (MAC: DD-AA-BB-88-12-43) replaced by another vAP 7502 having MAC address 11-22-33-44-55-66:

Note that the new AP 7502 device has the same configuration as the old AP 7502 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 radio1
  wlan theMOZART bss 1 primary
 interface radio2
  wlan theMOZART bss 1 primary
 interface ge1
  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 on page 1326.

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.

Note
WiNG access points only support one RF Domain, which is the **default** RF Domain. If needed, use this command to override the built-in default RF Domain configuration.

WiNG 7.1.X Interoperability with WiNG 5.9.X

Interoperability with access points running the WiNG 5.9.X OS is another salient feature of the WiNG 7.1.X OS. As part of this inter-interoperability, WiNG 7.1.X wireless controllers and service platforms will be able to deploy and manage the following WiNG 5.9.X APs:

- Access Points - AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP763, AP7662, AP8163, AP8543, AP8533.

The following output shows both WiNG 5.9.X and WiNG 7.1.X APs adopted to a WiNG 7.1.X NX9500 service platform:code

```
nx9500-6C8809#show version
NX9500 version 7.1.2.0-08D
Copyright (c) 2004-2019 Extreme Networks, Inc. All rights reserved.
Booted from primary

nx9500-6C8809 uptime is 0 days, 00 hours 31 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#
```

```
nx9500-6C8809#show adoption status
-----------------------------------------------------------------------------------------
----
DEVICE-NAME    VERSION       CFG-STAT    MSGS  ADOPTED-BY    LAST-ADOPTION       UPTIME
-----------------------------------------------------------------------------------------
----
ap8432-070235  5.9.4.0-015D  configured   No  nx9500-6C8809  0 days 00:27:59  2 days
23:02:09
ap7562-84A224  5.9.4.0-015D  configured   No  nx9500-6C8809  0 days 00:27:57  38 days
14:34:24
ap7532-DF9A4C  5.9.4.0-015D  configured   No  nx9500-6C8809  0 days 00:31:02  15 days
14:25:44
ap505-134038   7.1.0.0-124D  configured   No  nx9500-6C8809  0 days 00:30:49  1 days
03:07:01
-----------------------------------------------------------------------------------------
----
Total number of devices displayed: 4
nx9500-6C8809#
```

Note
In a mixed deployment, with access points running both WiNG 7.1.X and WiNG 5.9.X firmware, we recommend that these APs be placed in separate RF Domains.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <RF-DOMAIN-NAME> – Specify a sub-string of the RF Domain name.

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-smartrf    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

no on page 611	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 24: RF-Domain Config Mode Commands

Command	Description
alias on page 464	Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed-string, etc. at the RF Domain level
channel-list on page 471	Configures the channel list advertised by radios
contact on page 472	Configures network administrator's contact information (needed in case of any problems impacting the RF Domain)
control-vlan on page 473	Configures VLAN for traffic control on a RF Domain
controller-managed on page 473	Configures the adopting controller or service platform as this RF Domain's manager
country-code on page 474	Configures the country of operation
geo-coordinates on page 475	Configures the longitude and latitude of the RF Domain in order to fix its exact geographical location on a map
layout	Configures layout information
location on page 477	Configures the physical location of an RF Domain
location-server on page 478	Configures an ExtremeLocation server on the selected RF Domain. This command is supported only on the NX 95XX and NX 96XX series service platforms.
location-tenantid on page 479	Configures the ExtremeLocation Tenant's account number
mac-name on page 480	Maps MAC addresses to names
override-smart-rf on page 481	Configures RF Domain level overrides for Smart RF
override-wlan on page 482	Configures RF Domain level overrides for a WLAN
sensor-server on page 484	Configures an AirDefense sensor server on this RF Domain
stats on page 485	Configures stats related settings on this RF Domain. These settings define how RF Domain statistics are updated.
timezone on page 486	Configures a RF Domain's geographic time zone
tree-node on page 487	Configures the hierarchical (tree-node) structure under which this RF Domain appears
use (rf-domain-config-mode) on page 488	Enables the use of a specified Smart RF and/or WIPS policy with this RF Domain
no (rf-domain-config-mode) on page 490	Negates a command or reverts configured settings to their default

alias

Configures network, VLAN, host, string, network-service, etc. aliases at the RF Domain level

For information on aliases, see alias on page 172.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|igp|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 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)}
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 <ADRESS-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. • <ADRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. **Note:** Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. **Note:** 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.

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> [0|2] <LINE>
```

encrypted-string <ENCRYPTED-STRING-ALIAS-NAME>	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. • <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name. **Note:** Alias name should begin with '$'.

[0|2] <LINE>	Configures the value associated with the alias name specified in the previous step
	• [0|2] <LINE> – Configures the alias value
	
	Note, if password-encryption is enabled, in the `show > running-config` output, this clear text is displayed as an encrypted string, as shown below:
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`alias encrypted-string $enString 2 fABMK2is7UToNiZE3MQXbgAAA`
	`AxB0ZIysdqsEJwr6AH/Da//`
	`!`
	`--More--`
	`nx9500-6C8809`
	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:
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`!`
	`alias encrypted-string $enString 0 test11223344`
	`!`
	`--More--`
	`nx9500-6C8809`
	For more information on enabling password-encryption, see password-encryption on page 427.

```
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 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 on page 1534. • <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 sBqVCDAoxs3oByF5PCSuFAAA`
	`AAd7HT2+EiT/l/BXm9c4SBDv`
	`!`
	`alias hashed-string $PriMode 1 faffdde27cb49ad634ea20df4f`
	`7c8ef2685894d10ffcb1b2efba054112ecfc75`
	`--More--`
	`nx9500-6C8809`
	In the above `show > running-config` output, the '1' displayed before the hashed-string alias value indicates that the displayed text is hashed and not a clear text.

```
alias host <HOST-ALIAS-NAME> <HOST-IP>
```

host <HOST-ALIAS-NAME>	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. • <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 • <HOST-IP> – Specify the network host's IP address. Note: 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.

```
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
```

network <NETWORK-ALIAS-NAME>	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. • <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 • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. Note: 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.

```
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>	Creates a network-group alias for this RF Domain. Or associates an existing network-group alias with this RF Domain. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Note: Alias name should begin with '$'. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. Note: 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.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.

host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the hosts' IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.

```
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)}
```

alias network-service <NETWORK-SERVICE-ALIAS-NAME>	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. • <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. **Note:** Alias name should begin with '$'. **Note:** 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.
proto [<0-254>| <WORD>|eigrp|gre| igmp| igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – 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's) designated number is 17. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects *Enhanced Interior Gateway Routing Protocol* (EIGRP). The protocol number 88. • gre – Selects *Generic Routing Encapsulation* (GRE). The protocol number is 47. • igmp – Selects *Internet Group Management Protocol* (IGMP). The protocol number is 2. • igp – Selects *Interior Gateway Protocol* (IGP). The protocol number is 9. • ospf – Selects *Open Shortest Path First* (OSPF). The protocol number is 89. • vrrp – Selects *Virtual Router Redundancy Protocol* (VRRP). The protocol number is 112.
<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)}	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. • <1-65535> – Optional. Configures a destination port number from 1 - 65535 • <WORD> – Optional. Identifies the destination port by the service name provided. For example, the SSH service uses TCP port 22. • bgp – Optional. Configures the default *Border Gateway Protocol* (BGP) services port (179) • dns – Optional. Configures the default *Domain Name System* (DNS) services port (53) • ftp – Optional. Configures the default *File Transfer Protocol* (FTP) control services port (21) • ftp-data – Optional. Configures the default FTP data services port (20) • gopher – Optional. Configures the default gopher services port (70) • https – Optional. Configures the default HTTPS services port (443) • ldap – Optional. Configures the default *Lightweight Directory Access Protocol* (LDAP) services port (389) • nntp – Optional. Configures the default *Newsgroup* (NNTP) services port (119) • ntp – Optional. Configures the default *Network Time Protocol* (NTP) services port (123) • POP3 – Optional. Configures the default *Post Office Protocol* (POP3) 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 *Session Initiation Protocol* (SIP) services port (5060)
	• smtp – Optional. Configures the default *Simple Mail Transfer Protocol* (SMTP) 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 *Trivial File Transfer Protocol* (TFTP) 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 **Note:** The value referenced by alias $NUMBER, wherever used, is 100.

```
alias string <STRING-ALIAS-NAME> <LINE>
```

alias string <STRING-ALIAS-NAME>	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. • <VLAN-ALIAS-NAME> – Specify the string alias name. • <LINE> – Specify the string value. **Note:** Alias name should begin with '$'. **Note:** 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.

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

alias vlan <VLAN-ALIAS-NAME>	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. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. Note: Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094. Note: 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.

Examples

```
nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 7.1.0.0-010D

!
!
version 2.6
!
!
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--
nx9500-6C8809(config)#
```

In the following examples the global aliases '$kerberos' and '$TestVLANAlias' are associated with the RF Domain 'test' and overrides applied:

```
nx9500-6C8809(config-rf-domain-test)#alias network-service $kerberos proto tcp
749 750 80

nx9500-6C8809(config-rf-domain-test)#alias vlan $TestVLANAlias 10

vnx9500-6C8809(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
nx9500-6C8809(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.

```
nx9500-6C8809(config)#alias network-group $test host 192.168.1.10 192.168.1.11
nx9500-6C8809(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.

```
nx9500-6C8809(config-rf-domain-test)#alias network-group $test host 192.168.10.10
nx9500-6C8809#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
nx9500-6C8809(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

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
channel-list [2.4GHz|5GHz|5GHZ-Hi|5GZ-Lo|dynamic]
channel-list dynamic
channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
channel-list 5GHz-Hi <CHANNEL-LIST>
channel-list 5GHz-Lo <CHANNEL-LIST>
```

Parameters

```
channel-list dynamic
```

dynamic	Configure this setting to enable the dynamic channel listing mode for smart scans in the 2.4 and 5 GHz bands. This setting is disabled by default.

```
channel-list 5GHz-Hi <CHANNEL-LIST>
```

5GHz-Hi <CHANNEL-LIST>	In case of AP510i/e and AP56i/h access points functioning in the dual 5GHz mode, use this command to configure the channel list advertised by radios operating in 5GHz high frequency band mode. • <CHANNEL-LIST> – Specify the list of channels (100 - 165) separated by commas or hyphens. Note: Formoreinformation on the software modes supported on the AP510i/e and AP560i/h model access points, see rf-mode on page 1129.

```
channel-list 5GHz-Lo <CHANNEL-LIST>
```

5GHz-Lo <CHANNEL-LIST>	In case of AP510i/e and AP56i/h access points functioning in the dual 5GHz mode, use this command to configure the channel list advertised by radios operating in 5GHz low frequency band mode. • <CHANNEL-LIST> – Specify the list of channels (36 - 64) separated by commas or hyphens. Note: Formoreinformation on the software modes supported on the AP510i/e and AP560i/h model access points, see rf-mode on page 1129.

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 (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (rf-domain-config-mode) on page 490	Disables the VLAN designated for controlling RF Domain traffic

controller-managed

Configures the RF Domain manager as the adopting controller.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
controller-managed
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-rf-domain-test)#controller-managed
```

```
nx9500-6C8809(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
nx9500-6C8809(config-rf-domain-test)#
```

Related Commands

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
nx9500-6C8809(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

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

Parameters

```
geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

geo-coordinates <-90.0000-90.0000> <-180.0000-180.0000>	Configures the geo-coordinates of this RF Domain • <-90.0000-90.0000> – Specify the latitude from -90.0000 - 90.0000. • -180.0000-180.0000 – Specify the longitude from -180.0000 - 180.0000.

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

no (rf-domain-config-mode) on page 490	Removes or resets this RF Domain's configured geo-coordinates

layout

Configures the RF Domain'sayout 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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 • <AREA-NAME> – Specify the area name. After configuring the RF Domain's area of functioning, optionally specify the floor name (and number), description, and/or the location on map.
description <LINE>	Configures a description for this RF Domain • <LINE> – Specify a description that enables you to identify the RF Domain. For a multi-worded string, use double quotes.
floor <FLOOR-NAME> <1-4094>	Configures the RF Domain's layout in terms of the floor name and number • <FLOOR-NAME> – Specify the floor name. • <1-4094> – Optional. Specifies the floor number from 1 - 4094. The default floor number is 1. After configuring the RF Domain's floor name (and number), optionally specify the area name, description, and/or the location on map.
map-location <URL> units [feet|meters]	Configures the location of the RF Domain on the map • <URL> – Specify the URL to configure the map location. • units [feet|meters] – Configures the map units. The options are: feet or meters feet – Configures the map units in terms of feet meters – Configures the map units in terms of meter After configuring the location of the RF Domain on the map, optionally specify the area name, floor name (and number), and/or description.

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

no (rf-domain-config-mode) on page 490	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 an RF Domain policy.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
location <WORD>
```

Parameters

```
location <WORD>
```

location <WORD>	Configures the RF Domain location by specifying the area or building name • <WORD> – Specify the location.

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

no (rf-domain-config-mode) on page 490	Removes the RF Domain's location configuration

location-server

Configures the ExtremeLocation server's hostname on the RF Domain. When configured, RF Domain access points use a Websocket to forward 802.11 frames and BLE beacons to the specified ExtremeLocation server.

Starting with WiNG 7.1.2, AP5XX APs will not use WIPS to collect WiFi packets and BLE (iBeacons and Eddystone) beacons. The information will be collected in the Collector Table and forwarded to the ExtremeLocation server from the Collector Table.

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:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
location-server 1 ip <EL-SERVER-IP/HOSTNAME> {port <1-65535>}
```

Parameters

```
location-server 1 ip <IP/HOSTNAME> {port <1-65535>}
```

location-server 1 ip <IP/HOSTNAME>	Identifies the ExtremeLocation server by its hostname • 1 – Sets the server ID as 1. As of now only one ExtremeLocation server is configurable. • ip <IP/HOSTNAME> – Enter ExtremeLocation server's hostname. This is the ExtremeLocation server designated to receive RSSI scan data from a WiNG dedicated sensor. Note: 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.
port <1-65535>	Optional. Configures the port where the ExtremeLocation server is reachable. • <1-65535> – Specify a port from 1 - 65535. Note: By default, the ExtremeLocation server is reachable on port 443.

Examples

```
nx9500-6C8809(config-rf-domain-test)#location-server 1 ip feeds.extremelocation.com port
200
nx9500-6C8809(config-rf-domain-test)#show context
rf-domain test
 no country-code
 location-server 1 ip feeds.extremelocation.com port 200
nx9500-6C8809(config-rf-domain-test)#
```

Enabling Data (WiFi and BLE Beacons) forwarding to the ExtremeLocation Server

1 Configure sensor policy.

```
nx9500-6C8809(config-sensor-policy-ble)#rssi-interval-duration 35
```

2 In the RF Domain context:

a Use the sensor policy.

```
nx9500-6C8809(config-rf-domain-test)#use sensor-policy ble
```

b Configure the ExtremeLocation server hostname.

```
nx9500-6C8809(config-rf-domain-test)#location-server 1 ip feeds.extremelocation.com
```

c Configure the ExtremeLocation TenantID.

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#location-tenantid 1234
```

Related Commands

no (rf-domain-config-mode) on page 490	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, data (802.11 frames and/or BLE beacons) pushed to the ExtremeLocation server, include the Tenant's account number along with the reporting RF Domain manager's MAC address. Including the Tenant account number reinforces the Tenant's identity.

Note
For information on enabling data forwarding to the ExtremeLocation server, see location-server on page 478.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
location-tenantid <WORD>
```

Parameters

```
location-tenantid <WORD>
```

location-tenantid <WORD>	Configures the ExtremeLocation Tenant's account number • <WORD> – Specify the account number.

Examples

```
nx9500-6C8809(config-rf-domain-ExLocTenant1)#location-tenantid 123456

nx9500-6C8809(config-rf-domain-ExLocTenant1)#show context
rf-domain ExLocTenant1
 country-code us
 location-tenantid 123456
nx9500-6C8809(config-rf-domain-ExLocTenant1)#
```

Related Commands

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <MAC> – Specify the MAC address • <NAME> – Specify the client name for the specified MAC address. The name specified here will be used in events and statistics.

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

no (rf-domain-config-mode) on page 490	Removes the MAC address to name mapping

nsight-sensor

Enables the use of sensor module by NSight. This option is disabled by default.

Note

This option is not supported on the AP5XX model access points.

Supported in the following platforms:

- Access Points — AP7632, AP7662, AP8163, AP8432, AP8533
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX900

Syntax

```
nsight-sensor
```

Parameters

```
none
```

Examples

```
nx9500-6C8809(config-rf-domain-Test)#nsight-sensor
nx9500-6C8809(config-rf-domain-Test)#show context
nsight-sensor
nx9500-6C8809(config-rf-domain-Test)#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

Parameters

```
override-smartrf channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>
```

override-smartrf	Enables dynamic channel switching for Smart RF radios
channel-list	Configures a list of channels for 2.4 GHz and 5.0 GHz Smart RF radios
2.4GHz <CHANNEL-LIST>	Selects the 2.4 GHz Smart RF radio channels • <CHANNEL-LIST> – Specify a list of channels separated by commas.
5GHz <CHANNEL-LIST>	Selects the 5.0 GHz Smart RF radio channels • <CHANNEL-LIST> – Specify a list of channels separated by commas.

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 Ecospace floor Floor1 map-location www.firstfloor.com units meters
nx9500-6C8809(config-rf-domain-default)#
```

Related Commands

no (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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.
shutdown	Shuts down WLAN operation on all mapped radios
ssid <SSID>	Configures a override SSID associated with this WLAN • <SSID> – Specify the SSID (should not exceed 32 characters in length). 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.
template <TEMPLATE-NAME>	Configures a template name for this RF Domain • <TEMPLATE-NAME> – Specify the template name (should not exceed 32 characters in length).
vlan-pool <1-4094> {limit <0-8192>}	Configures the override VLANs available to this WLAN • <1-4094> – Specify the VLAN ID from 1 - 4094. • limit <0-8192> – Optional. Sets a limit to the number of users on this VLAN from 0 - 8192. The default is 0. 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.

```
override-wlan <WLAN-NAME> wpa-wpa2-psk [0 <WORD>|2 <WORD>]
```

<WLAN-NAME>	Configures the WLAN name. 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 <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 *Wi-Fi Protected Access* (WPA) and WEP. • <PASSPHRASE> – 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.

```
override-wlan <WLAN-NAME> wep128 [key <1-4> hex [0 <WORD>|2 <WORD>]|transmit-key <1-4>]
```

<WLAN-NAME>	Configures the WLAN name. 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. • <1-4> – Select the key index from 1- 4. • hex – Configures a hexadecimal key <WORD> – Specify the WEP128/Keyguard key (should not exceed 26 hexadecimal characters in length).
transmit-key <1-4>	Configures transmit WEP/Keyguard key settings • <1-4> – Transmit the key identified by the key index specified here. Specify the index from 1 - 4.

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 (rf-domain-config-mode) on page 490	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.

Access point radios can function as a sensor and upload information to a dedicated AirDefense server (external to the controller). Unique AirDefense 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. The access point works in conjunction with a dedicated AirDefense server forms a *Wireless Intrusion Protection System* (WIPS).

WIPS 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 acknowledgment of a threat.

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.

Note

Starting with the WiNG 7.2.0 release, AP5XX model access points are capable of capturing WPA3 frames in the sensor mode. For more information, see rf-mode on page 1129.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]}
```

Sensor-server <1-3>	Configures the AirDefense sensor server parameters • <1-3> – Select the server ID from 1 - 3. The server with the lowest defined ID is reached first. The default is 1.
ip <IP/HOSTNAME>	Configures the (non DNS) IPv4 address of the sensor server • <IP/HOSTNAME> – Specify the sensor server's IPv4 address or hostname.
port [443|<1-65535>]	Optional. Configures the sensor server port. The options are: • 443 – Configures port 443, the default port used by the AirDefense server • <1-6553> – Allows you to select a WIPS/AirDefense sensor server port from 1 - 65535

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-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

sensor-server on page 484	Disables the AirDefense sensor server parameters

stats

Configures settings that define how RF Domain statistics are updated

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 [<5-300>|auto]	Configures the interval at which RF Domain statistics are updated. The options are: • <5-300> – Specify an update interval from 5 - 300 seconds. • auto – The RF Domain manager automatically adjusts the update interval based on the load. This is the default setting.

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-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 (rf-domain-config-mode) on page 490	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 1299 (device config mode).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (rf-domain-config-mode) on page 490	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • campus-description - Provide a brief decription of the campus.
city	Configures the city for this RF Domain • city-description - Provide a brief description of the city.
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

```
ap505-13403B(config-rf-domain-default)#tree-node campus SanJoseUniversity
city SanJose country us
ap505-13403B(config-rf-domain-default)#show context
rf-domain default
 country-code us
 tree-node country us city SanJose campus SanJoseUniversity
ap505-13403B(config-rf-domain-default)#t
```

Related Commands

no (rf-domain-config-mode) on page 490	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.

Syntax

```
use [ble-data-export-policy|database-policy|license|nsight-policy|
rtl-server-policy|sensor-policy|smart-rf-policy|wips-policy]
use [ble-data-export-policy <POLICY-NAME>|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 [ble-data-export-policy <POLICY-NAME>|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: ble data export policy, database policy, NSight policy, sensor policy, Smart RF policy, WIPS policy. It also applies a Web filtering license to the selected RF Domain.
ble-data-export-policy <POLICY-NAME>	Associates a BLE data export policy with this RF Domain • <POLICY-NAME> – Specify the BLE data export policy name (should be existing and configured). When associated, access points within the RF Domain send BLE data to an external, third-party locationing-server using a Websocket and REST API. The BLE data export policy provides the external, locationing-server's URL. For more information on configuring the BLE data export policy, see ble-data-export-policy on page 216.
database-policy <DATABASE-POLICY-NAME>	Associates a database policy with the selected RF Domain • <DATABASE-POLICY-NAME> – Specify the database policy name (should be existing and configured). Note: This feature is not supported on the AP5XX model access points.
license <WEB-FILTERING-LICENSE>	Obtains the specified Web filtering license from the adopting controller • <WEB-FILTERING-LICENSE> – Specify the WEBF license name.

nsight-policy <NSIGHT-POLICY-NAME>	Associates an NSight policy with the selected RF Domain • 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.
rtl-server-policy <RTL-SERVER-POLICY-NAME>	Associates an *Real Time Locationing* (RTL) server policy with the selected RF Domain • <RTL-SERVER-POLICY-NAME> – Specify the RTL server policy name (should be existing and configured
sensor-policy <SENSOR-POLICY-NAME>	Associates a sensor policy with the selected RF Domain • <SENSOR-POLICY-NAME> – Specify the sensor policy name (should be existing and configured).
smart-rf-policy <SMART-RF-POLICY-NAME>	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. • <SMART-RF-POLICY-NAME> – Specify the Smart RF policy name (should be existing and configured). Note: SMART RF is only applicable on AP510i/e and AP560i/h functioning in the dual-5GHz mode. That is, on the AP, RF mode for both radios is set to WLAN-5GHz.
wips-policy <WIPS-POLICY-NAME>	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. • <WIPS-POLICY-NAME> – Specify the WIPS policy name (should be existing and configured).

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 (rf-domain-config-mode) on page 490	Removes policies associated 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|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 [ble-data-export-policy|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)#
```

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 75XX, 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 on page 611	Removes a NX 5500 series service platform from the network

nx7500

Adds an integrated NX7500 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 — NX7500, NX9500, NX9600, VX9000

Syntax

```
nx75xx <DEVICE-NX75XX-MAC>
```

Parameters

```
nx75xx <DEVICE-NX75XX-MAC>
```

<DEVICE-NX75XX-MAC>	Specifies the MAC address of the NX7500 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    MSGS 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

no	Removes an NX7500 series service platform from the network

nx9000

Adds an NX9500 series service platform to the network

Supported in the following platforms:

- Service Platforms — NX9500, NX9600, VX9000

Syntax

```
nx9000 <DEVICE-NX9XXX-MAC>
```

Parameters

```
nx9000 <DEVICE-NX9XXX-MAC>
```

<DEVICE-NX9000-MAC>	Specifies the MAC address of a NX9500 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

no on page 611	Removes a NX9500 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 a policy with the specified name 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:
  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)#
```

Related Commands

no on page 611	Removes an existing roaming-assist-policy

Note
For more information on the Roaming Assist Policy commands, Roaming Assist Policy on page 1858.

role-policy

Creates a role-based firewall policy and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
role-policy <ROLE-POLICY-NAME>
```

Parameters

```
role-policy <ROLE-POLICY-NAME>
```

<ROLE-POLICY-NAME>	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 on page 611	Removes an existing role policy

Note
For more information on Role Policy commands, see Role Policy on page 1602.

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 — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing dynamic BGP route map

routing-policy

Creates a routing policy and enters its configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing routing policy

Note
For more information on Routing Policy commands, see Routing Policy on page 1750.

rtl-server-policy

Creates an RTL server policy and enters its configuration mode. When configured and applied on an access point, 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 505, AP510
- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9600, VX9000

Syntax

```
rtl-server-policy <RTL-POLICY-NAME>
```

Parameters

```
rtl-server-policy <RTL-POLICY-NAME>
```

<RTL-POLICY-NAME>	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)#
```

no on page 611	Removes an existing RTL server policy
use (profile/device-config-mode-commands) on page 1247	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.
use (rf-domain-config-mode) on page 488	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 25: RTL Server Policy Config Mode Commands

Command	Description
url on page 498	Configures the RTL server's URL
no (rtl-server-policy-config-mode-commands) on page 498	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>
```

url <URL>	Configures the RTL server's URL • <URL> – Specify the URL.

Examples

```
nx9500-6C8809(config-rtl-server-policy-test)#url https://testrtlsever.com
nx9500-6C8809(config-rtl-server-policy-test)#show context
rtl-server-policy test
 url https://testrtlsever.com
nx9500-6C8809(config-rtl-server-policy-test)#
```

Related Commands

no (rtl-server-policy-config-mode-commands) on page 498	Removes the RTL server's configured URL

no (rtl-server-policy-config-mode-commands)

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>
```

no <URL>	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://testrtlsever.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)#
```

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 — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
schedule-policy <SCHEDULE-POLICY-NAME>
```

Parameters

```
schedule-policy <SCHEDULE-POLICY-NAME>
```

schedule-policy <SCHEDULE-POLICY-NAME>	Specify the Schedule policy name. If a policy with the specified name 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

no on page 611	Removes an existing schedule policy

schedule-policy-config-commands

The following table summarizes schedule-policy configuration mode commands:

Table 26: Schedule Policy Config Mode Commands

Command	Description
description on page 500	Configures a description for this schedule policy that differentiates it from other policies with similar time rule configurations
time-rule on page 501	Configures a time rule specifying the days and optionally the start and end times
no (schedule-policy-config-mode-commands) on page 502	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 — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures this schedule policy's description • <WORD> – Enter a description not exceeding 80 characters in length. The description should uniquely identify the policy from other policies with similar configuration.

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

no (schedule-policy-config-mode-commands) on page 502	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 195.

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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 • sunday – Applicable on Sundays only • monday – Applicable on Mondays only • tuesday – Applicable on Tuesdays only • wednesday – Applicable on Wednesdays only • thursday – Applicable on Thursdays only • friday – Applicable on Fridays only • saturday – Applicable on Saturdays only • weekends – Applicable on weekends only • weekdays – Applicable on weekdays only • all – Applicable on all days

start-time <HH:MM> [end-time <HH:MM>]	After specifying the days of enforcement, specify the following:
	• start-time – Optional. Specifies the enforcement start time
	  • <HH:MM> – Specify the start time in hours and minutes in the HH:MM format.
	If no start time is specified, the time rule is enforced, on the specified days, at all time.
	• end-time – Specifies the enforcement end time
	  • <HH:MM> – Specify the time in hours and minutes in the HH:MM format.

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 (schedule-policy-config-mode-commands) on page 502	Removes the time-rule from the schedule policy

no (schedule-policy-config-mode-commands)

Removes the selected schedule policy's settings

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

self

Invokes the logged device's configuration context

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 75XX, 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

  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-sensor-policy-test)#
```

Related Commands

no on page 611	Removes an existing sensor policy

sensor-policy-config-commands

The following table summarizes sensor-policy configuration mode commands:

Table 27: Sensor Policy Config Mode Commands

Command	Description
custom-scan on page 505	Configures the channel scanning settings when the scan-mode is set to custom-scan
rssi-interval-duration on page 506	Configures the interval at which dedicated sensors scan channels for RSSI assessments and send the collected data to a specified MPact server resource
scan-mode on page 506	Configures the mode of scanning used by dedicated sensors (access point radios)
no (sensor-policy-config-mode-commands) on page 507	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 506.

Supported in the following platforms:

- Service Platforms — NX 75XX, 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. • <CHANNEL-FREQUENCY> – Specify a single or multiple, 'comma-separated' channel frequencies.
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. • 20MHz – Sets the channel width as 20 Mhz • 40Mhz-Both – Sets the channel width as 40Mhz-Both • 40Mhz-Lowe – Sets the channel width as 40Mhz-Lower • 40Mhz-Upper – Sets the channel width as 40Mhz-Upper • 80Mhz – Sets the channel width as 80Mhz
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. • <SCAN-WEIGHT> – Specify the scan weightage given to each selected channel.

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 (sensor-policy-config-mode-commands) on page 507	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 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
rssi-interval-duration <1-60>
```

Parameters

```
rssi-interval-duration <1-60>
```

rssi-interval-duration <1-60>	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. • <1-60> – Specify the RSSI interval duration from 1 - 60 seconds. The default is 1 second. The channels scanned for RSSI assessment depends on the scan-mode selected. For more information, see scan-mode on page 506 and custom-scan on page 505. Ensure that the server's IP address or hostname has been configured in the access point sensor's RF Domain context.

Examples

```
nx9500-6C8809(config-sensor-policy-test)#rssi-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

no (sensor-policy-config-mode-commands) on page 507	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 75XX, 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>
```

scan-mode	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.
Channel-Lock lock-frequency <LOCK-FREQUENCY>	Configures the mode of scanning as channel-lock • lock-frequency <LOCK-FREQUENCY> – Locks scanning for RSSI data to one specific channel identified by the <LOCK-FREQUENCY> parameter. • <LOCK-FREQUENCY> – Specify the channel frequency in MHz. When specified, the sensor scans only this specified channel.

```
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 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 custom-scan on page 505.
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

no (sensor-policy-config-mode-commands) on page 507	Reverts the scan-mode to default (Default-Scan)

no (sensor-policy-config-mode-commands)

Removes or reverts to default a sensor policy's settings

Supported in the following platforms:

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

Syntax

```
no [custom-scan|rss1-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:

```
nx9500-6C8809nx9500-6C8809(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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
  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
  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

no on page 611	Removes an existing Smart RF policy

Note
For more information on Smart RF policy commands, see SMART-RF Policy on page 1638.

t5

Invokes the configuration mode of a t5 wireless controller

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
t5 <T5-DEVICE-MAC>
```

Parameters

```
t5 <T5-DEVICE-MAC>
```

t5 <T5-DEVICE-MAC>	Specify the T5 device's MAC address. The system enters the identified device's configuration mode. 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. After logging on to the T5 device, use the 'cpe' keyword and configure the following mandatory settings: • vlan – Set a VLAN from 1 - 4,094 used as a virtual interface for connections between the T5 controller and its managed CPE devices. • start ip – Set a starting IP address used in a range of addresses available to T5 controller connecting CPE devices. • end ip – Set an end IP address used in a range of addresses available to T5 controller connecting CPE devices.

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

no on page 611	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 594.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 with the specified name 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 on page 611	Removes an existing Web filter policy

web-filter-config-commands

The following table summarizes Web Filter policy configuration mode commands:

Table 28: Web Filter Config Mode Commands

Command	Description
cache-max-recs on page 512	Configures the maximum number of records (URLs and Web pages) cached in the local database
cache-save-interval on page 513	Configures the maximum time period for which a record (URL and Web page classification entry) is cached in the local database
logging on page 513	Configures the method used to log Web filtering events
server-host on page 514	Configures the URL classification server in case it is not the adopted controller
server-unreachable on page 515	Configures the action taken in case the classification server is unreachable
uncategorized-url on page 515	Configures the action taken in case the classification server fails to classify a URL/ Website
no (web-filter-policy-config-mode-commands) on page 516	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cache-max-recs <1-1000000>
```

Parameters

```
cache-max-recs <1-1000000>
```

cache-max-recs <1-1000000>	Specify the maximum number of records cached in the local database from 1 - 1000000. 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: • NX95XX – <1-1000000> (default is 100000) • NX75XX – <1-100000> (default is 10000) • RFS Switches – <1-10000> (default is 1000) • Access Points – <1-1500> (default is 500)

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

no (web-filter-policy-config-mode-commands) on page 516	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (web-filter-policy-config-mode-commands) on page 516	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
logging [logfile|syslog]
```

Parameters

```
logging [logfile|syslog]
```

logging [logfile|syslog]	Selects the method used to log Web filtering events. The options are: • logfile – Logs to a file. • syslog – Logs to the syslog server. This is the default setting.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • host-name <SERVER-HOST-NAME> – Identifies the classification server by its hostname. • ip-address <SERVER-IPv4> – Identifies the classification server by its IP address. • mint-id <SERVER-MiNT-ID> – Identifies the classification server by its MiNT ID.

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

no (web-filter-policy-config-mode-commands) on page 516	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
server-unreachable [block|pass]
```

Parameters

```
server-unreachable [block|pass]
```

server-unreachable [block|pass]	Configures the action taken in case the classification server is unreachable. The options are: • block – Denies access to the requested URL/Website • pass – Allows access to the requested URL/Website. This is the default value.

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 (web-filter-policy-config-mode-commands) on page 516	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • block – Denies access to the requested non-classified URL/Website • pass – Allows access to the requested non-classified URL/Website. This is the default value.

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 (web-filter-policy-config-mode-commands) on page 516	Reverts the action taken, in case the classification server fails to classify a URL/Website, to default (pass)

no (web-filter-policy-config-mode-commands)

Reverts the selected Web Filter policy settings to default, based on the parameters passed

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing WIPS policy

Note
For more information on WIPS Policy commands, see WIPS Policy on page 1663.

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.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

Parameters

```
wlan {<WLAN-NAME>|containing <WLAN-NAME>}
```

wlan <WLAN-NAME>	Configures a new WLAN • <WLAN-NAME> – Optional. Specify the WLAN name. Note: The WLAN name could be a logical representation of its coverage area (for example, engineering, marketing etc.). The name cannot exceed 32 characters.
containing <WLAN-NAME>	Optional. Configures an existing WLAN's settings • <WLAN-NAME> – 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.

Examples

```
nx9500-6C8809(config)#wlan wlan1
nx9500-6C8809(config-wlan-wlan1)#?
Wireless LAN Mode commands:
  802.11v                                 Configure 802.11v parameters
  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

no on page 611	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 29: WLAN Config Mode Commands

Command	Description
802.11v on page 523	Configures the IEEE 802.11v standard parameters on this WLAN
accounting (wlan-config-mode) on page 524	Defines a WLAN's accounting settings
acl on page 526	Defines the actions based on an ACL rule configuration
answer-broadcast-probes on page 527	Allows a WLAN to respond to probes for broadcast ESS
assoc-response on page 528	Configures a minimum *receive signal strength indication* (RSSI) value, below which the WLAN does not send a response to a client's association request
association-list on page 529	Attaches an existing global association list to a WLAN
authentication-type	Sets a WLAN's authentication type
bridging-mode on page 532	Configures how packets are bridged to/from this WLAN
broadcast-dhcp on page 533	Configures broadcast DHCP packet handling
broadcast-ssid on page 533	Advertises a WLAN's SSID in beacons
captive-portal-enforcement on page 534	Configures a WLAN's captive portal enforcement
client-access on page 535	Enables WLAN client access (normal data operations)
client-client-communication on page 535	Allows the switching of frames from one wireless client to another on a WLAN
client-load-balancing on page 535	Enables load balancing of WLAN clients

Table 29: WLAN Config Mode Commands (continued)

Command	Description
controller-assisted-mobility on page 537	Enables controller assisted mobility to determine wireless clients' VLAN assignment
data-rates on page 538	Specifies the 802.11 rates supported on the WLAN
description on page 540	Sets a WLAN's description
downstream-group-addressed-forwarding on page 540	Enables forwarding of downstream packets addressed to a group
dpi on page 541	Enables extraction of metadata flows on the WLAN
dynamic-vlan-assignment on page 542	Configures dynamic VLAN assignment on this WLAN
eap-types on page 543	Configures client access based on eap-type used for authentication
encryption-type on page 544	Sets the WLAN's encryption type
enforce-dhcp on page 546	Drops packets from clients with a static IP address
fast-bss-transition on page 546	Configures support for 802.11r fast BSS transition on a WLAN
http-analyze on page 547	Enables HTTP URL analysis on the WLAN
ip (wlan-config-mode) on page 549	Configures IPv4 settings on this WLAN
ipv6 (wlan-config-mode) on page 550	Configures IPv6 settings on this WLAN
kerberos on page 551	Configures Kerberos authentication parameters
mac-authentication on page 552	Configures MAC authentication parameters
nsight on page 553	Enables retention of guest client history in the NSight database
opendns on page 554	Configures the device ID, which is embedded in each DNS query packet going out from an access point, wireless controller, or service platform to the OpenDNS server
protected-mgmt-frames on page 555	Enables and configures the WLAN's frame protection mode and security association
proxy-arp-mode on page 556	Enables the proxy ARP mode for ARP requests
proxy-nd-mode on page 557	Configures the proxy ND mode for this WLAN member clients as either strict or dynamic
qos-map on page 558	Enables support for 802.11u QoS map element and frames
radio-resource-measurement on page 558	Enables support for 802.11k radio resource measurement
radius on page 559	Configures RADIUS parameters
registration on page 561	Configures settings enabling dynamic registration of devices. Use this command to specify the mode of registration and to configure corresponding parameters.
relay-agent on page 564	Enables support for DHCP relay agent information (option 82) feature on this WLAN
service (wlan-config-context) on page 565	Invokes service commands applicable in the WLAN configuration mode

Table 29: WLAN Config Mode Commands (continued)

Command	Description
shutdown on page 570	Shuts down a WLAN
ssid on page 571	Configures the WLAN's SSID
t5-client-isolation on page 572	Disallows clients connecting to the WLAN to communicate with one another
t5-security on page 573	Configures T5 PowerBroadband security settings
time-based-access on page 574	Configures time-based client access
use (wlan-config-mode) on page 575	Defines WLAN mode configuration settings
vlan on page 579	Assigns a VLAN for the WLAN
vlan-pool-member on page 580	Adds a member VLAN to the pool of VLANs for a WLAN
wep128 on page 581	Configures WEP128 parameters
wep64 on page 582	Configures WEP64 parameters
wing-extensions on page 583	Enables support for WiNG specific extensions to 802.11
wireless-client on page 585	Configures the transmit power for wireless clients transmission
wpa-wpa2 on page 588	Modifies TKIP and CCMP (WPA/WPA2) related parameters
no (wlan-config-mode) on page 590	Negates a command or reverts settings to their default

802.11v

Use this command to configure 802.11v parameters on this WLAN. The *IEEE 802.11* family of standards includes the 802.11v standard that allows client devices to exchange information about the network topology, including information about the *RF* environment, making each client network aware, facilitating overall improvement of the wireless network.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
802.11v [bss-transition|session-information-url <URL>]
```

Parameters

```
802.11v [bss-transition|session-information-url <URL>]
```

802.11v	Configures IEEE 802.11v parameters, such as 'bss-transition' and session-information-url'.
bss-transition	Enables BSS *(Base station Subsystem)* transition management capabilities on the WLAN APs. When enabled, WLAN APs send *BSS Transition Management Request* frames to 802.11v capable clients. These request frames suggest a specific AP, or a set of APs to which the client can transition to for better throughput and QoS *(Quality of Service)*. Note: This feature is disabled by default.
session-information-url <URL>	Configures the session information URL. This is the URL containing specific information about the client session. This is the URL to which the WLAN AP sends the BSS Transition Management Request frames. • <URL> - Specify the session information URL.

Examples

```
NOC-NX9500(config-wlan-test)#802.11v bss-transition

NOC-NX9500(config-wlan-test)#show context
wlan test
 ssid test123
 bridging-mode local
 encryption-type none
 authentication-type none
 802.11v bss-transition
NOC-NX9500(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Disables 802.11v BSS Transition Management capabilities and removes the session-information-url

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. When enabled, the WLAN uses an external RADIUS resource for accounting. This option is disabled by default. Use the `use > aaa-policy > <AAA-POLICY-NAME>` 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 • <IP/HOSTNAME> – Specify the IP address or name of the destination host.
port <1-65535>	Optional. Configures the syslog server's UDP port (this port is used to connect to the server) • <1-65535> – Specify the port from 1 - 65535. Default port is 514.
proxy-mode [none|through-controller|through-rf-domain-manager]	Optional. Configures the request proxying mode • none – Requests are directly sent to the server from the device • through-controller – Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device • through-rf-domain-manager – Proxies requests through the local RF Domain manager

```
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 delimitors (AABBCCDDEEFF)

pair-colon	Configures the MAC address format with pair-colon delimitors (AA:BB:CC:DD:EE:FF)
pair-hyphen	Configures the MAC address format with pair-hyphen deli mi tors (AA-BB-CC-DD-EE-FF). This is the default setting.
quad-dot	Configures the MAC address format with quad-dot deli mi tors (AABB.CCDD.EEFF)

case [lower|upper]	The following keywords are common to all:
	• case – Specifies MAC address case (upper or lower)
	  • lower – Specifies MAC address is filled in lower case (for example, aa-bb-cc-dd-ee-ff)
	  • upper – Specifies MAC address is filled in upper case (for example, AA-BB-CC-DD-EE-FF)

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 (wlan-config-mode) on page 590	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 *Access Control Lists* (ACLs) 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 *Access Control Entries* (ACEs). 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 action taken based on an ACL rule configuration (for example, drop a packet) • exceed-rate – Action is taken when the rate exceeds a specified value
wireless-client-denied-traffic <0-1000000>	Sets the action to deny traffic to the wireless client when the rate exceeds the specified value • <0-1000000> – Specify a allowed rate threshold of disallowed traffic in packets/sec. 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.
blacklist <0-86400>	Optional. Sets the time period for which an offending wireless client is blacklisted. • <0-86400> – Configures the blacklist duration from 0 - 86400 seconds. Offending clients are re-authenticated once the blacklist duration, configured here, is over.
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 (wlan-config-mode) on page 590	Removes the action (de-authenticate or blacklist) to be taken when an associated client exceeds the thresholds configured for storm traffic

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
answer-broadcast-probes
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-wlan-1)#answer-broadcast-probes
nx9500-6C8809(config-wlan-1)#
```

Related Commands

no (wlan-config-mode) on page 590	Does not allow this WLAN to respond to probe requests that do not specify a SSID

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <1-12> – Specify the deny-threshold from 1 - 12.
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 • <-100--40> – Specify a value from -100 - -40 dBm.

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

no (wlan-config-mode) on page 590	Removes the configured deny-threshold and rssi-threshold values

association-list

Attaches an existing global association list with this WLAN. For more information on global association lists, see global-association-list on page 367.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

Parameters

```
association-list global <GLOBAL-ASSO-LIST-NAME>
```

association-list global <GLOBAL-ASSO-LIST-NAME>	Attaches an existing global association list with this WLAN • <GLOBAL-ASSO-LIST-NAME> – Specify the global association list name (should be existing and configured).

Examples

```
nx9500-6C8809(config-wlan-test)#association-list global my-clients
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 bridging-mode tunnel
 encryption-type none
 authentication-type none
 association-list global my-clients
nx9500-6C8809(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Removes the global association list associated with this WLAN

authentication-type

Sets the WLAN's mode of authentication

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none|sae|sae-psk]
```

Parameters

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none|sae|sae-psk]
```

authentication-type	Configures a WLAN's authentication type The authentication types are: **EAP**, **EAP-MAC**, **EAP-PSK**, **Kerberos**, **MAC**, **SAE** , **SAE-PSK**, and **none**.
eap	Configures EAP authentication (802.1X) 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. 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. 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. 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 *Temporal Key Integrity Protocol* (TKIP) or Counter Mode with *Cipher Block Chaining Message Authentication Code Protocol* (CCMP) encryption types. 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. 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) 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 *Network Time Protocol* (NTP) for synchronizing the clocks of its *Key Distribution Center* (KDC) server(s).

mac	Configures MAC authentication (RADIUS lookup of MAC address) MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP. 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. MAC authentication can only identify devices, not users. 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
sae	Enables WPA3-Personal (SAE Authentication) on this WLAN. Note: SAE authentication is only supported with **mandatory** protected management frames. For more information, see protected-mgmt-frames on page 555. WPA3 is the latest security protocol developed by the WiFi Alliance as part of its series of *Wi-Fi Protected Access* (WPA) protocols. It is has stronger configuration, authentication, and encryption features. WPA3 is more secure and protects against offline brute force attacks that WPA2 could not provide. WPA3 offers two levels of protection: WPA3-Personal (with 128-bit encryption) and WPA3-Enterprise (with 192-bit encryption). WPA3-Personal uses *Simultaneous Authentication of Equals* (SAE) authentication method. SAE was first defined in the IEEE 802.11s standard for authentication between 802.11s enabled mesh peers. SAE is a zero-knowledge proof key exchange protocol that uses finite group cryptography. The client and access point go through an SAE handshake to negotiate a fresh *Pairwise Master Key* (PMK). This PMK is used in a traditional four-way handshake to generate a session key. Note: The 32-byte PMK negotiated through the SAE handshake cannot be guessed using offline dictionary attacks, even though it is later used in a four-way handshake. Enable this option to allow only WPA3-capable clients authenticate with the access point and access the wireless network.
sae-psk	Enables WPA3-Compatibility mode. Use this option to enable WPA2 in addition with WPA3-Personal. When enabled, both WPA3-capable and WPA2-capable clients can authenticate with the access point and access the wireless network. Note: SAE-PSK authentication is supported with **optional** management frames. For more information, see protected-mgmt-frames on page 555.

Examples

```
nx9500-6C8809(con fig-wlan-test)#authentication-type eap

nx9500-6C8809(con fig-wlan-test)#show context
wlan test
 said test
 bridging-mode tunnel
 encryption-type none
authentication-type eap
 accounting slog host 172.16.10.4 port 2
```

```
 cal exceed-rate wireless-client-denied-traffic 20 disassociate
nx9500-6C8809(con fig-wlan-test)#

ap505-13403B(config-wlan-test)#authentication-type sae-psk

ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type gcmp256
 authentication-type eap
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 use aaa-policy test
 http-analyze syslog host 10.234.160.4 port 21 proxy-mode through-controller
 controller-assisted-mobility
 opendns device-id 0014AADF8EDC6C59
 dpi metadata http
ap505-13403B(config-wlan-test)#

nx9500-6C8809(config-wlan-SAEAuth)#authentication-type sae

nx9500-6C8809(config-wlan-SAEAuth)#show context
wlan SAEAuth
 ssid sae
 vlan 203
 bridging-mode local
 encryption-type ccmp
 authentication-type sae
 protected-mgmt-frames mandatory
 wpa-wpa2 psk 0 12345678
nx9500-6C8809(config-wlan-SAEAuth)#
```

Related Commands

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
broadcast-ssid
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-wlan-1)#broadcast-ssid
nx9500-6C8809(config-wlan-1)#
```

Related Commands

no (wlan-config-mode) on page 590	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 (wlan-config-mode) on page 575.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fall-back}
```

captive-portal-enforcement	Enables captive portal enforcement on a WLAN. This option is disabled by default.
fall-back	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

no (wlan-config-mode) on page 590	Disables captive portal enforcement

client-access

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-access
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-wlan-1)#client-access
nx9500-6C8809(config-wlan-1)#
```

Related Commands

no (wlan-config-mode) on page 590	Disables WLAN client access

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-client-communication
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-wlan-1)#client-client-communication
nx9500-6C8809(config-wlan-1)#
```

Related Commands

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
client-load-balancing {allow-single-band-clients|band-discovery-intvl|
capability-ageout-time|max-probe-req|probe-req-invl}
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 [2.4GHz|5GHz]	Optional. Allows single band clients to associate even during load balancing • 2.4GHz – Enables load balancing across 2.4 GHz channels • 5GHz – Enables load balancing across 5.0 GHz channels This option is enabled by default for 2.4 and 5.0 GHz bands.
band-discovery-intvl <0-10000>	Optional. Configures time interval to discover a client's band capability before connection • <0-10000> – Specify a value from 0 - 10000 seconds. The default is 10 seconds.
capability-ageout-time <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. • <0-10000> – Specify a value from 0 - 10000 seconds. The default is 3600 seconds.

```
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 • 2.4GHz – Configures maximum client probe requests on 2.4 GHz radios • 5GHz – Configures maximum client probe requests on 5.0 GHz radios • <0-10000> – Specify a client probe request threshold from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 60.
probe-req-intvl 2.4GHz|5GHz] <0-10000>	Optional. Configures client probe request interval limits for device association • 2.4GHz – Configures the client probe request interval on 2.4 GHz radios • 5GHz – Configures the client probe request interval on 5.0 GHz radios • <0-10000> – Specify a value from 0 - 10000. The default for both 2.4 and 5.0 GHz radios is 10 seconds.

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
controller-assisted-mobility
```

Parameters

```
None
```

Examples

```
ap505-13403B(config-wlan-test)#controller-assisted-mobility
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type ccmp
 authentication-type sae-psk
 protected-mgmt-frames optional
 controller-assisted-mobility
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Disables controller or service platform assisted mobility to determine a wireless client's VLAN assignment

data-rates

Configuration the 802.11 rates supported on this WLAN

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|basic-mcs-1s|basic-mcs0-7|mcs-1s|mcs-2s|mcs-3s|
mcs0-15|mcs0-23|mcs0-7|mcs16-23|mcs8-15|mcs8-23]

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|
basic-mcs0-7|mcs-1s|mcs2s|mcs3s|mcs4s|mcs0-15|mcs0-23|mcs0-7|mcs16-23|mcs8-15|mcs8-23]
```

Parameters

```
data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]
```

data-rates	Specifies the 802.11 rates supported when mapped to a 2.4 GHz radio
b-only	Uses rates that support only 11b clients
bg	Uses rates that support both 11b and 11g clients
bgn	Uses rates that support 11b, 11g and 11n clients
default	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 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|basic-mcs-1s|basic-mcs0-7|mcs-1s|mcs-2s|
mcs-3s|mcs0-15|mcs0-23|mcs0-7|mcs16-23|mcs8-15|mcs8-23]
```

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'). 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: • 1 – 1-Mbps • 11 – 11-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps
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: • 12 – 12 Mbps • 18 – 18-Mbps • 24 – 24 Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • basic-1 – basic 1-Mbps • basic-11 – basic 11-Mbps • basic-12 – basic 12-Mbps • basic-18 – basic 18-Mbps • basic-2 – basic 2-Mbps • basic-36 – basic 36-Mbps • basic-48 – basic 48-Mbps • basic-5.5 – basic 5.5-Mbps • basic-54 – basic 54-Mbps • basic-6 – basic 6-Mbps • basic-9 – basic 9-Mbps • basic-mcs-1s – Modulation and coding scheme data rates for 1 Spatial Stream • mcs-1s – Applicable to 1-spatial stream data rates • mcs-2s – Applicable to 2-spatial stream data rates • mcs-3s – Applicable to 3-spatial stream data rates

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wlan-config-mode) on page 590	Removes the 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
downstream-group-addressed-forwarding
```

Parameters

```
None
```

Examples

```
ap505-13403B(config-wlan-test)#downstream-group-addressed-forwarding
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type ccmp
 authentication-type sae-psk
 dynamic-vlan-assignment allowed-vlans 1-3
 protected-mgmt-frames optional
 controller-assisted-mobility
 dpi metadata http
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dpi metadata [http|ssl|tcp-rtt|voice-video]
```

Parameters

```
dpi metadata [http|ssl|tcp-rtt|voice-video]
```

dpi metadata [http|ssl|tcp-rtt|voice-video]	Enables extraction of the following metadata flows: • http – 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. • ssl – 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 • tcp-rtt – 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. • voice-video – 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.

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

no (wlan-config-mode) on page 590	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 on page 579. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 alias on page 172 .

Examples

```
ap505-13403B(config-wlan-test)#dynamic-vlan-assignment allowed-vlans 2,3,4
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type ccmp
 authentication-type sae-psk
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames optional
 controller-assisted-mobility
 dpi metadata http
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 [allow|deny]	Configures a list of allowed or denied EAP types • allow – Configures a list of EAP types allowed for WLAN client authentication • deny – Configures a list of EAP types not allowed for WLAN client authentication
[aka|all|fast|peap|sim| tls|ttls]	The following EAP types are common to the 'allow' and 'deny' keywords: • aka – Configures EAP *Authentication and Key Agreement* (AKA) and EAP-AKA' (AKA Prime). EAP-AKA is one of the methods in the EAP authentication framework. It uses *Universal Mobile Telecommunications System* (UMTS) and *Universal Subscriber Identity Module* (USIM) for client authentication and key distribution. • all – Allows or denies usage of all EAP types on the WLAN • fast – Configures EAP *Flexible Authentication via Secure Tunneling* (FAST). EAP-FAST establishes a *Transport Layer Security* (TLS) tunnel, to verify client credentials, using *Protected Access Credentials* (PAC). • peap – Configures *Protected Extensible Authentication Protocol* (PEAP). PEAP or Protected EAP uses encrypted and authenticated TLS tunnel to encapsulate EAP. • sim – Configures EAP *Subscriber Identity Module* (SIM). EAP-SIM uses *Global System for Mobile Communications* (GSMC) SIM for client authentication and key distribution. • 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. • ttls – Configures *Tunneled Transport Layer Security* (TTLS). EAP-TTLS is an extension of TLS. Unlike TLS, TTLS does not require every client to generate and install a CA- signed certificate. • 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.

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

no (wlan-config-mode) on page 590	Reverts to default setting - eap-types allow all

encryption-type

Sets the WLAN's encryption type

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
encryption-type [ccmp|gcmp256|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

Parameters

```
encryption-type [ccmp|gcmp256|keyguard|none|tkip-ccmp|wep128|web128-keyguard|wep64]
```

encryption-type	Configures the WLAN's data encryption parameters
ccmp	Configures *Advanced Encryption Standard Counter Mode CBC-MAC Protocol* (AES-128CCM/CCMP)
gcmp256	Configures AES-GCM *(Advanced Encryption Standard-Galois Counter Mode)* protocol (WPA3-Enterprise 192-bit) encryption mode. GCMP-256 is a block cipher which works on 256-bit blocks. Note: GCMP encryption is only supported with eap authentication-type. For more infromation, see authentication-type on page 529. Note: GCMP encryption is only supported with mandatory protected management frames. For more information, see protected-mgmt-frames on page 555.
keyguard	Configures Keyguard *Mobile Computing Mode* (MCM)
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)#

ap505-13403B(config-wlan-test)#encryption-type gcmp256

ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type gcmp256
 authentication-type eap
```

```
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 use aaa-policy test
 controller-assisted-mobility
 dpi metadata http
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (wlan-config-mode) on page 590	Disables dropping of packets from clients with a static IP address

fast-bss-transition

Enables or disables support for 802.11r *Fast-BSS Transition* (FT) 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • over-ds – Optional. Enables 802.11r client roaming over the *Distribution System* (DS). 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.

Examples

```
nx9500-6C8809(config-wlan-test)#fast-bss-transition
nx9500-6C8809(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 (wlan-config-mode) on page 590	Disables support for 802.11r FT on the WLAN

http-analyze

Enables HTTP URL analysis on the WLAN

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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/HOSTNAME>	Forwards client and URL information to a syslog server • host <IP/HOSTNAME> – Specify the syslog server's IP address or hostname
port <1-65535>	Optional. Specifies the UDP port to connect to the syslog server from 1 - 65535
proxy-mode [none|through-controller| through-rf-domain-manager]	Optional. Specifies if the request is to be proxied through another device • none – Requests are sent directly to syslog server from device • through-controller – Proxies requests through the wireless controller configuring the device • through-rf-domain-manager – Proxies the requests through the local RF Domain manager

Examples

```
ap505-13403B(config-wlan-test)#http-analyze syslog host 10.234.160.4 port 21 proxy-mode
through-controller
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type gcmp256
 authentication-type eap
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 use aaa-policy test
 http-analyze syslog host 10.234.160.4 port 21 proxy-mode through-controller
 controller-assisted-mobility
 dpi metadata http
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Disables HTTP URL analysis on the WLAN

ip (wlan-config-mode)

Configures IPv4 settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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-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
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
 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 (wlan-config-mode) on page 590	Resets IP ARP or DHCP trust parameters to default. ARP trust is disabled, ARP mismatch verification is enabled, or DHCP trust is disabled.

ipv6 (wlan-config-mode)

Sets the DHCPv6 and ICMPv6 *neighbor discovery* (ND) components for this WLAN

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|nd]
ipv6 dhcpv6 trust
ipv6 nd [header-mismatch-validation|raguard|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|raguard|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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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: • 0 <LINE> – Configures a clear text password • 2 <LINE> – Configures an encrypted password • <LINE> – Specify the password.

```
kerberos realm <REALM>
```

kerberos	Configures a WLAN's Kerberos authentication parameters 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 The parameters are: password, realm, and server.
server [primary|secondary]	Configures the primary and secondary KDC server parameters • primary – Configures the primary KDC server parameters • secondary – Configures the secondary KDC server parameters

host <IP/HOSTNAME>	Sets the primary or secondary KDC server address • <IP/HOSTNAME> – Specify the IP address or name of the KDC server.
port <1-65535>	Optional. Configures the UDP port used to connect to the KDC server • <1-65535> – Specify the port from 1 - 65535. The default is 88.

```
kerberos server timeout <1-60>
```

kerberos	Configures a WLAN's Kerberos authentication parameters The parameters are: password, realm, and server.
timeout <1-60>	Modifies the Kerberos KDC server's timeout parameters • <1-60> – Specifies the wait time for a response from the Kerberos KDC server before retrying. Specify a value from 1 - 60 seconds.

Examples

```
nx9500-6C8809(config-wlan-test)#kerberos server timeout 12
nx9500-6C8809(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

no (wlan-config-mode) on page 590	Removes Kerberos authentication related parameters on the 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 nsight-policy (global-config-mode) on page 418.

Related Commands

no (wlan-config-mode) on page 590	Disables client-history retention in the NSight database

opendns

Configures the per-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 on page 91.

Syntax

```
opendns device-id <DEVICE-ID>
```

Parameters

```
opendns device-id <DEVICE-ID>
```

opendns device-id <DEVICE-ID>	Configures the device ID to embed in DNS queries sent to OpenDNS • <DEVICE-ID> – Specify the device ID.

Examples

The following command fetches the device_id from the OpenDNS site.

```
ap505-13403B(#opendns ApiToken 9110B39543DEB2ECA1F473AE03E8899C00019073
device_id = 0014AADF8EDC6C59
ap505-13403B(#
```

Use this device_id in the WLAN configuration context.

```
ap505-13403B((config)#wlan opendns
ap505-13403B((config-wlan-opendns)#opendns device-id 0014AADF8EDC6C59
ap505-13403B((config-wlan-opendns)#commit
ap505-13403B((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

no (wlan-config-mode) on page 590	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 *security association* (SA) 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. The *Protected management frames* (PMF) protocol only applies to robust management frames after establishment of *Robust Security Network association Pairwise Transient Key* (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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 frame protection is mandatory or optional. **Note:** Frame protection mode is disabled by default.
mandatory	Enforces PMF on this WLAN (management frames are always protected). **Note:** This option does not allow non-PMF capable clients to associate.

optional	Provides PMF only for those clients that support PMF (that is, management frame protection is optional). Note: This option allows both PMF-capable and non-PMF capable wireless clients to associate. However, only the management frames of PMF-capable clients is protected.
sa-query [attempts <1-10>| timeout <100-1000>]	Configures the following SA parameters: • attempts <1-10> – Configures the number of SA query attempts from 1 - 10. The default is 5. • timeout <100-1000> – 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.

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • dynamic – Forwards ND request to wireless for which a response could not be proxied. This is the default value. • strict – Does not forward ND requests to the wireless side

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • hybrid – Optional. Uses the hybrid model of smart-rf neighbors and roaming frequency to neighbors

Examples

```
ap505-13403B(config-wlan-test)#radio-resource-measurement neighbor-report hybrid
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type gcmp256
 authentication-type eap
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 radio-resource-measurement neighbor-report hybrid
 use aaa-policy test
 http-analyze syslog host 10.234.160.4 port 21 proxy-mode through-controller
 controller-assisted-mobility
 opendns device-id 0014AADF8EDC6C59
 dpi metadata http
ap505-13403B(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Disables support for 802.11k radio resource measurement capabilities (IEEE 802.11k) on this WLAN

radius

Configures RADIUS related parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *change of authorization* (CoA) messages, which affect session authorization, or *disconnect messages* (DM) that terminate a session immediately. This option is disabled by default.
nas-identifier <NAS-ID>	Configures the *network access server* (NAS) 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. • <NAS-ID> – Specify the NAS identifier attribute (should not exceed 256 characters in length).
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. • <NAS-PORT-ID> – Specify the NAS port ID attribute (should not exceed 256 characters in length). 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.
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 vlan/vlan-pool-member options (in the WLAN config mode) is used. 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.

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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. For more information on enabling the EGuest server, see eguest-server (VX9000 only) on page 987 (profile config mode). For more information on configuring an EGuest deployment, see configuring ExtremeGuest captive portal on page 267.
send-mode [https|https|udp]	Optional. Specifies the protocol used to forward registration requests to the external AAA policy servers. The options are: • HTTPS – Sends registration requests as HTTPS packet • HTTP – Sends registration requests as HTTP packet • UDP – Sends registration requests as UDP packet, using the UPD port 12322. This is the default setting.

```
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}	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. • none – Optional. Requests are sent directly to the controller from the requesting device • through-controller – Optional. Requests are proxied through the controller configuring the device • through-rf-domain-manager – Optional. Requests are proxied through the local RF Domain manager • 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. After specifying the proxy-mode, optionally specify the protocol used to send the requests to the external registration server host.
send-mode [https|https|udp]	Optional. Specifies the communication protocol used. The options are; • HTTPS – Sends registration requests as HTTPS packets • HTTP – Sends registration requests as HTTP packets • UDP – Sends registration requests as UDP packet, using the UPD port 12322. This is the default setting.

```
registration [device|device-OTP|user] group-name <RAD-GROUP-NAME>
{agreement-refresh <0-144000>|expiry-time <1-43800>}
```

registration	Configures dynamic guest registration and validation parameters. This option is disabled by default.
[device|device-OTP| user]	Configures the mode used to register guest users of this WLAN. Options include device, external, user, and device-OTP • 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 *one-time-passcode* (OTP)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. • 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 *MAC authentication*. • user – Registers guest users using one of the following options: e-mail address, mobile-number, or member-id. 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.
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. • <RAD-GROUP-NAME> – Specify the RADIUS group name (should not exceed 64 characters).
expiry-time <1-43800>	Optional. Configures the amount of time, in hours, before registered addresses expire and must be re-entered • <1-43800> – Specify a value from 1 - 43800 hrs. The default is 1500 hrs.
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. • <0-100> – Specify a value from 0 - 144000. The default is 0 minutes.

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *Lightweight DHCPv6 Relay Agent* (LDRA) 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: • circuit ID suboption – Provides the SNMP port interface index • remote ID – Provides the controller's MAC address
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

```
ap505-13403B(config-wlan-test)#relay-agent dhcp-option82
ap505-13403B(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode local
 encryption-type ccmp
 authentication-type mac
 dynamic-vlan-assignment allowed-vlans 2-4
 protected-mgmt-frames mandatory
 protected-mgmt-frames sa-query attempts 1
 use aaa-policy test
 relay-agent dhcp-option82
 http-analyze syslog host 10.234.160.4 port 21 proxy-mode through-controller
 controller-assisted-mobility
 opendns device-id 1222222222222356
 dpi metadata http
ap505-13403B(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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
service [accounting-migration-on-roaming|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-deauth-on-roam-detection|unresponsive-client|wpa-wpa2|show]

service accounting-migration-on-roaming

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 accounting-migration-on-roaming
```

accounting-migration-on-roaming	Enables migration of accounting session information and data usage details from one AP to another for roaming clients. When a client roams from AP1 to AP2, accounting for the client stops on AP1 and is resumed only after AP2 authenticates with the accounting server. By enabling this feature, accounting session information and data usage details migrates to the new AP, and the AP does not have to re-authenticate with the accounting server. Note: Accounting session information is supported on all WiNG APs. In case of controllers, this feature is valid only when APs use the controller as a proxy.

```
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 Passpoint Policy on page 1817.
cred-cache [clear-on-4way-timeout| clear-on-disconnect]	Clears credential cache based on the parameter passed • clear-on-4way-timeout – Clears cached client credentials after the 4way handshake with a client has timed out. This option is enabled by default. • clear-on-disconnect – Clears cached client credentials after the client has disconnected from the network. This option is disabled by default.
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	Validates the Predictive real-time *Pairwise Master Key Identifier* (PMKID) contained in a client's association request against the one present in the wpa-wpa2 handshake. This option is enabled by default. This functionality is based on the *Proactive Key Caching* (PKC) extension of the 802.11i EEEE standard. Whenever a wireless client successfully authenticates with a AP it receives a *Pairwise Master Key* (PMK). 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.
radio-crypto	Uses radio hardware for encryption and decryption. This is applicable only for devices using *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* (CCMP) 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. • <0-254> – Specify a value from 0 - 254. This default value is 0.

```
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. • <1-4> – Select a index from 1 - 4. The default value is 1.

```
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 vlan <1-4094>	Enables adoption failure monitoring on an adopted AP. Also configures a adoption failover VLAN. This feature is disabled by default. • VLAN <1-4094> – Specify the VLAN on which clients are placed when the connectivity between the AAP and the controller is lost. 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. 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. 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).
captive-portal external-server	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. 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.

```
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. Use the *crm* 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. Use the *crm* keyword to specify the DNS server to monitor.

crm <RESOURCE-NAME>	This keyword is common to the 'dhcp' and 'dns' parameters. • crm – Identifies the DHCP and/or DNS server to monitor • <RESOURCE-NAME> – Specify the name of the DHCP or DNS server. 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.
vlan <1-4094>	This keyword is common to the 'dhcp' and 'dns' parameters. After specifying the DHCP/DNS sever resource, specify the failover VLAN. • VLAN <1-4094> – Configures the failover VLAN from 1 - 4094. 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. 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.

```
service unresponsive-client [attempts <1-1000>|ps-detect {threshold <1-1000>}|
timeout <1-60>]
```

unresponsive	Configures handling of unresponsive clients
attempts <1-1000>	Configures the maximum number of successive packets that failed transmission • <1-1000> – Specify a value from 1 - 1000. The default is 7.
ps-detect {threshold <1-1000>}	Enables the detection of power-save mode clients, whose PS stats has not been updated on the AP. This option is enabled by default. • threshold – Optional. Configures the threshold at which power-save client detection is triggered • <1-1000> – Configures the number of successive unacknowledged packets received before power-save detection is triggered. Specify a value from 1 - 1000. The default is 3.
timeout <1-60>	Configures the interval, in seconds, for successive packets not acknowledged by the client • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.

Examples

```
nx9500-6C8809(config-wlan-test)#service allow-ht-only
nx9500-6C8809(config-wlan-test)#service monitor aaa-server
nx9500-6C8809(config-wlan-test)#service accounting-migration-on-roaming
nx9500-6C8809(config-wlan-test)#show context
wlan test
 ssid test
 vlan 1
 bridging-mode tunnel
 encryption-type none
```

```
 authentication-type none
 service accounting-migration-on-roaming
 service monitor aaa-server
 service allow-ht-only
 controller-assisted-mobility
nx9500-6C8809(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Removes or reverts to default WLAN settings configured using the 'service' command

shutdown

Shuts down a WLAN. The 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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	Shuts down the WLAN when specified events occur. Disabled by default.
on-critical-resource <CR-NAME>	Optional. Shuts down the WLAN when critical resource failure occurs. Disabled by default. • <CR-NAME> – Specifies the name of the critical resource being monitored for this WLAN.
on-meshpoint-loss	Optional. Shuts down the WLAN when the root meshpoint link fails (is unreachable). Disabled by default.
on-primary-port-link-loss	Optional. Shuts down the WLAN when a device losses its primary Ethernet port (ge1/up1) link. Disabled by default.
on-unadoption	Optional. 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
```

```
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
 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

no (wlan-config-mode) on page 590	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 the WLAN's SSID

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (wlan-config-mode) on page 590	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 the 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 75XX, 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

no (wlan-config-mode) on page 590	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 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 the 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 75XX, 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) • <STRING> – Specify the hex password (should not exceed the 10 - 26 characters).
passphrase <STRING>	Configures the passphrase shared by both transmitting and receiving authenticators • <STRING> – 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.

```
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 *wpa-enterprise* and *wpa-personal* keywords: • [ccmp|tkip|tkip-ccmp] – Applies one of the following encryption algorithms to the T5 support WLAN configuration: **CCMP**, **TKIP**, or **TKIP-CCMP**.
version [mixed|wpa|wpa2]	The following parameters are common to the *wpa-enterprise* and *wpa-personal* keywords: • version – Applies one of the following encryption schemes to the vT5 support WLAN configuration: **WPA**, **WPA2**, or **mixed**.

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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • sunday – Allows access on Sundays only • monday – Allows access on Mondays only • Tuesdays – Allows access on Tuesdays only • wednesday – Allows access on Wednesdays only • thursday – Allows access on Thursdays only • friday – Allows access on Fridays only • saturday – Allows access on Saturdays only • weekends – Allows access on weekends only • weekdays – Allows access on weekdays only • all – Allows access on all days
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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|
purview-application-policy|roaming-assist-policy|url-filter|wlan-qos-policy]
use [aaa-policy <AAA-POLICY-NAME>|application-policy <APP-POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy <POLICY-
NAME>|
captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>|
```

```
purview-application-policy <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 <APP-POLICY-NAME>|
association-acl-policy <ASSOCIATION-POLICY-NAME>|bonjour-gw-discovery-policy <POLICY-
NAME>|
captive-portal <CAPTIVE-PORTAL-NAME>|passpoint-policy <PASSPOINT-POLICY-NAME>|
purview-application-policy <POLICY-NAME>|roaming-assist-policy <POLICY-NAME>|
url-filter <URL-FILTER-NAME>|wlan-qos-policy <WLAN-QOS-POLICY-NAME>]
```

aaa-policy <AAA-POLICY-NAME>	Uses an existing AAA policy with a WLAN • <AAA-POLICY-NAME> – Specify the AAA policy name.
association-acl <ASSOCIATION-POLICY-NAME>	Uses an existing association ACL policy with a WLAN • <ASSOCIATION-POLICY-NAME> – Specify the association ACL policy name.
application-policy <APP-POLICY-NAME>	Uses an existing application policy with the WLAN. WLAN traffic is inspected and access control and quality of service actions applied based on the rules defined in the application policy. • <APP-POLICY-NAME> - Specify the Application policy name. The policy should be existing and configured. Note: The WiNG 5.9.X enabled devices use a third-party, DPI engine to detect pre-defined application definitions. To enable AVC and app-usage stats reporting in a WiNG 5.9.X network, see application-group on page 191 and application-policy on page 195.
bonjour-gw-discovery-policy <POLICY-NAME>	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. 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. • <POLICY-NAME> – Specify the Bonjour GW Discovery policy name. Should be existing and configured.
captive-portal <CAPTIVE-PORTAL-NAME>	Specifies the captive-portal policy to use if enforcing captive-portal authentication on this WLAN • <CAPTIVE-PORTAL-NAME> – Specify the captive-portal policy name. Should be existing and configured.

passpoint-policy <PASSPOINT-POLICY-NAME>	Associates a passpoint policy (Hotspot2 configuration) with this WLAN. • <PASSPOINT-POLICY-NAME> – Specify the Passpoint policy name. Should be existing and configured. 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. Define one passpoint policy for every WLAN configured.
purview-application-policy <PURVIEW-APP-POLICY-NAME>	Uses an existing Purview application policy with the WLAN. WLAN traffic is inspected and access control and quality of service actions applied based on the rules defined in the Purview application policy. • <PURVIEW-APP-POLICY-NAME> - Specify the Purview Application policy name. The policy should be existing and configured. Note: The WiNG 7.1.X enabled devices use Extreme Networks' *EAA* (Purview™) DPI engine to detect pre-defined application definitions. To enable AVC in a WiNG 7.1.X network, see purview-application-group on page 432 and purview-application-policy on page 436.
roaming-assist-policy <POLICY-NAME>	Associates an existing roaming assist policy with this WLAN • <POLICY-NAME> – Specify the Roaming Assist policy name. Should be existing and configured.
url-filter <URL-FILTER-NAME>	Associates an existing URL list with this WLAN • <URL-FILTER-NAME> – Specify the URL filter name. Should be existing and configured.
wlan-qos-policy <WLAN-QOS-POLICY-NAME>	Uses an existing WLAN QoS policy with a WLAN • <WLAN-QOS-POLICY-NAME> – Specify the WLAN QoS policy name. Should be existing and configured.

```
use ip-access-list [in|out] <IP-ACCESS-LIST-NAME>
```

ip-access-list [in|out] <IP-ACCESS-LIST-NAME>	Applies an IP access list to incoming and outgoing packets • in – Applies the IP ACL to incoming packets • out – Applies IP ACL to outgoing packets • <IP-ACCESS-LIST-NAME> – Specify the IP access list name.

```
use ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>
```

ipv6-access-list [in|out] <IPv6-ACCESS-LIST-NAME>	Applies an IPv6 access list to incoming and outgoing packets • in – Applies the IPv6 ACL to incoming packets • out – Applies IPv6 ACL to outgoing packets • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name.

```
use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>
```

mac-access-list [in|out] <MAC-ACCESS-LIST-NAME>	Applies a MAC access list to incoming and outgoing packets. • in – Applies the MAC ACL to incoming packets • out – Applies MAC ACL to outgoing packets • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name.

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 *Access Control Entries* (ACEs). 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
nx9500-6C8809(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 (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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 alias on page 172.

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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 • <0-8192> – Specifies the number of users allowed

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 (wlan-config-mode) on page 590	Removes the list of VLANs mapped to a WLAN

wep128

Configures WEP128 parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-4> – Specify the key number from 1 - 4.
ascii [0 <WORD>| 2 <WORD>| <WORD>]	Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters
hex [0 <WORD>| 2 <WORD>| <WORD>]	Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures keys as 13 ASCII characters converted to hex, or 26 hexadecimal characters

```
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. • <WORD> – Specify a pass key from 4 - 32 characters.

```
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 • <1-4> – Specify a key index from 1 - 4.

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 313233343536373839616263 64
NOC-NX9500(config-wlan-test)#
```

Related Commands

no (wlan-config-mode) on page 590	Resets the WEP128 parameters to factory-default values.

wep64

Configures WEP64 parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 The parameters are: key, key-from-passkey, and transmit-key.
key <1-4>]	Configures pre-shared hex keys • <1-4> – Configures a maximum of four key indexes. Select a key index from 1 - 4.

ascii [0 <WORD>| 2 <WORD>| <WORD>]	Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128).
hex [0 <WORD>| 2 <WORD>| <WORD>]	Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures the key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)

```
wep64 keys-from-passkey <WORD>
```

keys-from-passkey <WORD>	Specifies a pass key from which keys are derived • <WORD> – Specify a pass key from 4 - 32 characters.

```
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 • <1-4> – Specify a key index from 1 - 4.

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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}	Enables support for AP attributes IE *(information element)* • include-hostname – Optional. When enabled, includes AP's hostname, as a sub-element, in the AP attributes IE. 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: • - Recognize Extreme APs • - Determine if the AP supports PAN BU features, irrespective of whether these features are enabled or not. AP attributes IE is not added to beacons and probe responses by default.
overage-hole-detection {11k-clients| offset <5-20>| threshold <-80--60>}	Enables *coverage hole detection* (CHD) 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 radio-resource-measurement on page 558. CHD is disabled by default. After enabling CHD, optionally configure the following parameters: • 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. • offset <5-20> – Optional. Configures the offset added to the threshold to obtain the access point's signal strength (as seen by the client) considered adequate. • <5-20> – Specify the offset value from 5 - 20. The default is 5. • 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. • <-80--60> – Specify the threshold from -80 - -60 dBm. The default is -70 dBm.
ft-over-ds-aggregate	Enables *fast-transition* (FT) 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 *distribution system* (DS) 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.

move-command	Enables use of *Hyper Fast Secure Roaming* (HFSR) for clients on this WLAN. This feature applies only to certain client devices. This option is disabled by default.
scan-assist {channel-info-interval <6-9>}	Enables support for scanning assist. When enabled, allows faster roams on *Dynamic Frequency Selection* (DFS) channels by eliminating passive scans. Clients get channel information directly from possible roam candidates. This option is disabled by default. • channel-info-interval <6-9> – Optional. Configures the interval at which channel information is periodically retrieved from potential roam candidates without requesting scan assist. • <6-9> – Specify the interval from 6 - 9 seconds. When enabled, the default value is 8 seconds.
smart-scan	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.
wing-load-information	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.
wmm-load-information	Enables support for WiNG *Wi-Fi MultiMedia* (WMM) Load Information Element in radio transmissions with legacy clients. This option is disabled by default.

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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <0-256> – Specify a value from 0 - 256.
cred-cache-ageout <60-86400>	Configures the timeout period for which client credentials are cached across associations • <60-86400> – Specify a value from 60 - 86400 seconds.
hold-time <1-86400>	Configures the time period for which wireless client state information is cached post roaming • <1-86400> – Specify a value from 1 - 86400 seconds.
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. • <60-86400> – Specify a value from 60 - 86400 seconds.
max-firewall-sessions <10-10000>	Configures the maximum firewall sessions allowed per client on a WLAN • <10-10000> – Specify the maximum number of firewall sessions allowed from 10 - 10000.
reauthentication <30-86400>	Configures periodic reauthentication of associated clients • <30-86400> – Specify the client reauthentication interval from 30 - 86400 seconds.
t5-inactivity-timeout <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. • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 60 seconds.

tx-power <0-20>	Configures the transmit power indicated to clients • <0-20> – Specify a value from 0 - 20 dBm.
vlan-cache-ageout <60-86400>	Configures the timeout period for which client VLAN information is cached across associations. • <60-86400> – Specify a value from 60 - 86400 seconds.

```
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
nx9500-6C8809(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

no (wlan-config-mode) on page 590	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *Wi-Fi Protected Access II* (WPA2) 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 *Pairwise Master Key* (PMK) 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 • <1-5> – Specify a value from 1 - 5. The default is 2.

init-wait <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. • <5-1000000> – Specify a value from 5 - 1000000 microseconds.
priority [high|normal]	Configures the relative priority of handshake messages compared to other data traffic • high – Treats handshake messages as high priority packets on a radio. This is the default setting. • normal – Treats handshake messages as normal priority packets on a radio
timeout <10-5000> <10-5000>	Configures the timeout period, in milliseconds, for a handshake message to retire. Once this period is exceeded, the handshake message is retired. • <10-5000> – Specify a value from 10 - 5000 millisceonds. The default is 500 milliseconds. • <10-5000> – Optional. Configures a different timeout between the second and third attempts'

```
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 <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. • <30-86400> – Specify a value from 30 - 86400 seconds.
unicast <30-86400>	Configures a periodic interval for the rotation of keys, used for unicast traffic. This option is disabled by default. • <30-86400> – Specify a value from 30 - 86400 seconds.

```
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 • <0-65535> – Specify a value from 0 - 65536 seconds. <0-65535> – Specify a value from 0 - 65535 seconds. The default is 60 seconds.

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 (wlan-config-mode) on page 590	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

Syntax

```
no <PARAMETERS>
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes this WLAN's 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

```
nx9500-6C8809(config-wlan-test)#no ?
  802.11v                                Configure 802.11v parameters
  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                Do not 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                    Reset the authentication to use on
                                         this wlan to default (none/Pre-shared
                                         keys)
  broadcast-dhcp                         Configure broadcast DHCP packet
                                         handling
  broadcast-ssid                         Do not advertise the SSID of the WLAN
                                         in beacons
  captive-portal-enforcement             Configure how captive-portal is
                                         enforced on the wlan
  client-access                          Disallow client access on this wlan
                                         (no data operations)
  client-client-communication            Disallow switching of frames from one
                                         wireless client to another on this
                                         wlan
  client-load-balancing                  Disable load-balancing of clients on
                                         this wlan
  controller-assisted-mobility           Disable configure assisted mobility
  data-rates                             Reset data rate configuration to
                                         default
  description                            Reset the description of the wlan
  downstream-group-addressed-forwarding  Disable downstream group addressed
                                         forwarding of packets
  dpi                                    Deep-Packet-Inspection (Application
                                         Assurance)
  dynamic-vlan-assignment                Dynamic VLAN assignment configuration
  eap-types                              Allow all EAP types on this wlan
  encryption-type                        Reset the encryption to use on this
                                         wlan to default (none)
  enforce-dhcp                           Drop packets from Wireless Clients
                                         with static IP address
  fast-bss-transition                    Disable 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
  nsight                                 Nsight Server
  opendns                                OpenDNS related config for this wlan
  protected-mgmt-frames                  Disable support for Protected
                                         Management Frames (IEEE 802.11w)
  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                                 Disable the 802.11u QoS map element
                                          and frame
  radio-resource-measurement              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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 611	Removes an existing WLAN QoS POLICY

Note
For more information on WLAN QoS policy commands, see WLAN-QoS Policy on page 1685.

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 *Internet service provider* (ISP) 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 on page 511 .

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 on page 604.

Note

URL filtering is a licensed feature. Procure and install the license in the device configuration mode. For more information, see license on page 1280 (device config mode).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
url-filter <URL-FILTER-NAME>
```

Parameters

```
url-filter <URL-FILTER-NAME>
```

<URL-FILTER-NAME>	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

Sl 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

Sl No.	Category Type	Category
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
11	Social and Photo Sharing	Social Networking
12	Software Update	N/A

Sl 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

no on page 611	Removes an existing URL filter policy

url-filter-config-commands

The following table summarizes URL filter configuration mode commands:

Table 30: URL Filter Config Mode Commands

Command	Description
blacklist on page 597	Creates a blacklist rule defining a list of banned Websites and URLs
blockpage on page 599	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
description on page 601	Configures an appropriate description for this URL filter
whitelist on page 602	Creates a whitelist rule defining a list of Websites and URLs allowed access by clients.
no (url-filter-config-mode-commands) on page 603	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 on page 594.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <SELECT-CATEGORY-TYPE>	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 created with the URL List and added to the database. 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 Select 'all' to blacklist all category-types. Some of the category-types are further classified into categories. For example, the 'adult-content' category-type is differentiated into the following categories: • alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons. The system blocks all categories (URLs falling within their limits) within the selected category-type.
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>	Associates a URL list with this URL filter. When associated with a blacklist rule, all URLs listed in the specified URL list are blacklisted. 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 url-list on page 604 . • <URL-LIST-NAME> – Enter URL list name (should be existing and configured)
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

no (url-filter-config-mode-commands) on page 603	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 form 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]
```

blockpage path [external|internal]	Specifies if the location of the page displayed, to the client when a requested URL is blocked, is external or internal • external – Indicates the page displayed is hosted on an external Web server resource. If selecting this option, use the `blockpage > external > url <URL>` command to provide the path to the external Web server hosting the page. • internal – Indicates the page displayed is hosted internally. This is the default setting. If selecting this option, use the `blockpage > internal > <SELECT-PAGE-TYPE> > <LINE/IMAGE-URL>` command to define the page configuration.

```
blockpage external url <URL>
```

blockpage external url <URL>	Configures the URL of the external Web server hosting the page (displayed to the client when a requested URL is blocked). • url <URL> – Specify the URL of the Web server and the blocking page name Valid URLs should begin with http:// or https:// The URL can contain query strings. Use '&' or '?' character to separate field-value pair. Enter 'ctrl-v' followed by '?' to configure query strings

```
blockpage internal [content|footer|header|main-logo|org-name|org-signature|
small-logo|title] <LINE/IMAGE-URL>
```

blockpage internal [content|footer|header|main-logo|org-name|org-signature| small-logo|title] <LINE/IMAGE-URL>	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 • content – Configures the text (message) displayed on the blocking page • footer – Configures the text displayed as the blocking page footer • header – Configures the text displayed as the blocking page header • org-name – Configures the organization's name displayed on the blocking page • org-signature – Configures the organization's signature displayed on the blocking page • title – Configures the title of the blocking page. • main-logo – Configures the location of the main logo (organization's large logo) • small-logo – Configures the location of the small logo (organization's small logo) The following keyword is common to all of the above parameters: • <LINE/IMAGE-URL> – 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.

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

no (url-filter-config-mode-commands) on page 603	Removes the blocking page configurations

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (url-filter-config-mode-commands) on page 603	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	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 created with the URL List and added to the database. 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. Select 'all' to whitelist all category-types. Some of the category-types are further classified into categories. For example, the 'adult-content' category-type is differentiated into the following categories: • alcohol-tobacco, dating-personals, gambling, nudity, pornography-sexually-explicit, sex-education, and weapons. The system allows all categories (URLs falling within their limits) within the selected category-type.
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>	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. 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 url-list on page 604. • <URL-LIST-NAME> – Enter URL list name (should be existing and configured)
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 (url-filter-config-mode-commands) on page 603	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 form the URL filter.

no (url-filter-config-mode-commands)

Use the no command to remove this URL filter's configured parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 611	Removes an existing URL list

url-list-config-commands

The following table summarizes URL list configuration mode commands:

Table 31: URL List Config Mode Commands

Command	Description
url on page 606	Adds URL entries to this URL list
description on page 606	Creates a blacklist rule defining a list of banned Web sites and URLs
no (url-list-config-mode-commands) on page 607	Removes this URL list's settings

url

Adds URL entries to this URL list

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
url <WORD> {depth <1-10>}
```

Parameters

```
url <WORD> {depth <1-10>}
```

url <WORD> {depth <1-10>}	Adds a URL entry • <WORD> – Specify the URL to add. • 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. <1-10> – Specify the depth from 1 - 10.

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 (url-list-config-mode-commands) on page 607	Removes a URL entry from this URL list

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (url-list-config-mode-commands) on page 607	Removes this URL list's description

no (url-list-config-mode-commands)

Removes this URL list's settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *virtual machine* (VM) 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

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 Poicy 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

no on page 611	Removes a VX 9000 wireless controller

no

Negates a command, or reverts configured settings to their default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [aaa-policy|aaa-tacacs-policy|alias|ap505|ap510|nx5500|nx75xx|nx9000|nx9600|
application|application-group|
application-policy|association-acl-policy|auto-provisioning-policy|bgp|ble-data-export-
policy|
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|purview-application-
group|
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|
ble-data-export-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|purview-
application-group|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 [ap510|ap505|ap560|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 [ap510|ap505|ap560|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 {ap7632|ap7662|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 NX9500 and NX9600 platforms:

```
no t5 <T5-DEVICE-MAC>

no bgp [as-path-list|community-list|extcommunity-list|ip-access-list|ip-prefix-list]
<LIST-NAME>

no route-map <ROUTE-MAP-NAME>
```

The following ‘no’ command is specific to the VX9000 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
  ap505                               Delete an AP505 access point
  ap510                               Delete an AP510 access point
  ap560                               Delete an AP560 access point
  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
  ble-data-export-policy              Delete a  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
  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
purview-application-group           Delete Purview application-group
purview-application-policy          Delete a Purview application policy
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
rest                                Remove the configured url
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 Configuratino
rssi-interval-duration              Configure the periodicity of sensding
                                    RSSI info from sensor to server
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)#
```

6 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 32: Common Commands

Command	Description
clrscr on page 616	Clears the display screen
commit on page 617	Commits (saves) changes made in the current session
exit on page 618	Ends and exits the current mode. In the Global cnfiguration mode, this command and moves to the PRIV EXEC mode.
help on page 618	Displays the interactive help system
no on page 620	Negates a command or reverts values to their default settings
revert on page 623	Reverts changes to their last saved configuration
service on page 623	Invokes service commands to troubleshoot or debug (config-if) instance configurations
show on page 674	Displays running system information
write on page 676	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
clrscr
```

Parameters

```
None
```

Examples

The following example shows the terminal window or screen before the clrscr command is executed:

```
ap505-13403B>device-upgrade ?
  DEVICE-NAME     Name/MAC address of device
  all             Upgrade all devices
  ap505           Upgrade AP505 Device
  ap510           Upgrade AP510 Device
  cancel-upgrade  Cancel upgrading the device
  containing      Specify devices that contain a sub-string in the hostname
  load-image      Load the device images to controller for device-upgrades
  rf-domain       Upgrade all devices belonging to an RF Domain

ap505-13403B>
ap505-13403B>clrscr [ENTER]
```

The terminal window or screen after the clrscr command is executed:

```
ap505-13403B>
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <WORD> – 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.
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>
nx9500-6C8809help 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 Configuratino
  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 on page 90	User Exec no command
no on page 160	Priv Exec no command
no on page 611	Global Config no command

revert

Reverts changes made, in the current session, to their last saved configuration

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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:

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 {<1-100000>}
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 *Network Operations Center* (NOC) server to adopted devices
request-full-config-from- adopter	Configures a request for full configuration updates from the adopter device In an *hierarchically managed* (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 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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <DOMAIN-NAME> – Specify the RF Domain name.

```
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. For more information on viewing logged looped packet information execute the `service > show > diag > pkts` command.

```
service clear dpi [all|app|app-category] stats {on <DEVICE-OR-DOMAIN-NAME>}
```

clear dpi	Clears *Deep Packet Inspection* (DPI) statistics 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: • all – Clears all DPI related (application and app-category) statistics • app – Clears only application related statistics • app-category – Clears only app-category related statistics
on <DEVICE-OR-DOMAIN-NAME>	Optional. Clears DPI statistics based on the parameters passed on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, controller, service platform, or RF Domain.

```
service clear file-sync history {on <DOMAIN-NAME>}
```

clear file-sync history	Clears client-bridge certificate synchronization statistics 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 • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 This command is applicable only on the NX 95XX and NX 96XX series service platforms.
on <DEVICE-NAME>	Optional. Clears history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform Note: When executing the clear virtual-machine-history command, provide the name of the service platform running the VMs.

```
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 • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
service clear wireless [ap|client] {<MAC>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

clear wireless [ap|client] statistics	Clears wireless statistics counters based on the parameters passed • ap statistics – Clears applicable AP statistics counters • client statistics – Clears applicable wireless client statistics counters
<MAC> {on <DEVICE-OR-DOMAIN-NAME>}	The following keywords are common to the 'ap' and 'client' parameters: • <MAC> – Optional. Clears statistics counters for a specified AP or client. Specify the AP/client MAC address. • on <DEVICE-OR-DOMAIN-NAME> – 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.

```
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>	Optional. Clears the Web filtering cache on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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>	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. • <1-3> – Optional. Specify the radio interface index, if not specified as part of the radio ID.
on <DEVICE-OR-DOMAIN-NAME>	Optional. This is a recursive parameter, which clears wireless radio statistics on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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>	Optional. This is a recursive parameter, which clears WLAN statistics on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
service clear xpath requests {<1-100000>}
```

clear xpath	Clears XPATH related information
requests	Clears pending XPATH get requests
<1-100000>	Optional. Specifies the session number (cookie from show sessions) • <1-100000> – Specify the session number from 1 - 100000. Note: Omits clearing the current session's pending XPATH get requests.

```
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|uf-8]	Selects a formatting layout or skin for CLI tabular outputs • ansi – Uses ANSI characters for borders • hashes – Uses hashes (#) for borders • minimal – Uses one horizontal line between title and data rows • none – Displays space separated items with no decoration • percent – Uses the percent sign (%) for borders • stars – Uses asterisks (*) for borders • thick – Uses thick lines for borders • thin – Uses thin lines for borders • utf-8 – Uses UTF-8 characters for borders
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>	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 database on page 66 (user/priv exec modes). • username <USER-NAME> – Configures database username • password <PASSWORD> – Configures a password for the username specified above 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 database-policy global config on page 299 and database-client-policy global-config on page 296.

```
service database authentication delete-user username <USER-NAME>
```

database	Performs database related actions 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 • username <USER-NAME> – Deletes the username identified by the <USER-NAME> keyword Once deleted, the database cannot be accessed using the specified combination of username and password.

```
service database start-shell
```

database	Performs database related actions 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 • <0-999> – Specify the number of off-line days from 0 - 999.
time <TIME>	Optional. Specifies the off-line time period. Access Points off-line for this period of time are deleted. • <TIME> – Specify the time in HH:MM:SS format.

```
service eguest remove-data [deleted-devices|offline-for days <0-999> {time <HH:MM:SS>}]
```

service eguets	Enables ExtremeGuest server data maintenance
remove-data	Removes offline and/or deleted devices from the ExtremeGuest server database Note: When enabled, the device configuration and database collection is removed permanently. Note: If a controller is removed, then its adopted APs are also removed,

deleted-devices	Removes deleted devices
offline-for days <0-999> {time <HH:MM:SS>}	Removes offline devices from the ExtremeGuest server database. Offline devices are devices that have not been reporting to the ExtremeGuest server for a specified number of days. Use this option to configure that threshold value. Devices that have not reported to the ExtremeGuest server for the number of days specified here are considered to be offline and removed. • days <0-999> – Specify the threshold, in days, from 0 - 999. • time <HH:MM:SS> – 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.

```
service eguest restore factory-default
```

eguest	Enables ExtremeGuest server data maintenance
restore factory-default	Reinitializes the ExtremeGuest server to factory-default settings. Use this option to stop the ExtremeGuest server and database. Note: Extreme caution is recommended, as this command deletes data related to ExtremeGuest server and database. Debug log files are also deleted.

```
service force-send-config {on <DEVICE-OR-DOMAIN-NAME>}
```

force-send-config	Resends configuration to device(s)
on <DEVICE-OR-DOMAIN-NAME>	Optional. Resends configuration to a specified device or all devices in a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <DEVICE-NAME> – Specify the name of the device.

```
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 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 *Comma-Separated Values* (CSV) or JSON *(JavaScript Object Notation)* format 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: • csv – Exports user data files in the CSV format • json – Exports user data files in the JSON format

<DEST-URL>	Configures the destination URL. The files are exported to the specified location. Both IPv4 and IPv6 address formats are supported. • IPv4 URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file • IPv6 URLs: tftp://<hostname|[IPv6]>[:port]/path/file ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]>/path/file
rfdomain <DOMAIN-NAME>	Optional. Filters user data based on RF Domain name. Only the filtered data are exported. • <DOMAIN-NAME> – Specify the RF Domain name.
wlan <WLAN-NAME>	Optional. Filters user data based on WLAN name. Only the filtered data are exported. • <WLAN-NAME> – Specify the WLAN name.
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. • 1-Day – Filters and exports previous day's data • 1-Month – Filters and exports previous month's data • 1-Week – Filters and exports previous week's data • 2-Hours – Filters and exports last 2 hours data • 30-Mins – Filters and exports last 30 minutes data • 5-Hours – Filters and exports last 5 hours data • all – Exports the entire database

```
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 • json – Imports user data files in the JSON format
<SOURCE-URL>	Configures the Source URL. The files are imported from the specified location. Both IPv4 and IPv6 address formats are supported. • IPv4 URLs: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file sftp://<user>:<passwd>@<hostname|IP>[:port]>/path/file • IPv6 URLs: tftp://<hostname|[IPv6]>[:port]/path/file ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file sftp://<user>:<passwd>@<hostname|[IPv6]>[:port]>/path/file

```
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 • <MAC> – Clears capability records of a specified client. Specify the client's MAC address in the AA-BB-CC-DD-EE-FF format. • all – Clears the capability records of all clients
on <DEVICE-NAME>	Optional. Clears client capability records on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • on <DEVICE-NAME> – Optional. Enables LEDs on a specified device • <DEVICE-NAME> – Specify name of the AP, wireless controller, or service platform.

```
service nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]
```

nsight clear-offline [all|offline-for days <0-999> {time <TIME>}]	Clears NSight data received from offline controllers, based on the parameters passed. Select one of the following options: • all – Clears NSight data received from all offline controllers • offline-for days <0-999> time <TIME> – Clears NSight data received from controllers that have been offline for a specified time period • days <0-999> – Specifies the number of days controllers have been offline <0-999> – Specify the number of days from 0 - 999 days. Select "0" to identify controllers offline less than 24 hours. time <TIME> – Optional. Specifies the total time for which controllers have been offline <TIME> – Specify the time in HH:MM:SS format. Note: This command is applicable only to the NX 95XX, NX 96XX, and VX 9000 platforms.

```
service radio <1-3> adaptivity
```

radio <1-3>	Configures radio parameters • <1-3> – Specify the radio index from 1 - 3.
adaptivity	Simulates the presence of interference on the current channel

```
service radio <1-3> channel-switch <36-196> [160|20|40|80|80-80]
```

radio <1-3>	Configures radio parameters • <1-3> – Specify the radio index from 1 - 3.
channel-switch <36-196> [160|20|40|80| 80-80]	Enables channel switching • <36-196> – Specifies the channel to switch to from 36 - 196. • 160|20|40|80|80-80] – Specifies the bandwidth for the above specified channel. Select the appropriate option.

```
service radio <1-3> dfs simulate-radar [extension|primary]
```

radio <1-3>	Configures radio parameters • <1-3> – Specify the radio index from 1 - 3.
dfs	Enables *Dynamic Frequency Selection* (DFS)
simulate-radar [extension|primary]	Simulates the presence of a radar on a channel. Select the channel type from the following options: • extension – Simulates a radar on the radio's current extension channel • primary – Simulates a radar on the radio's current primary channel

```
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. • test – Tests the RADIUS server's account with user provided parameters
[<IP>|<HOSTNAME>]	Sets the RADIUS server's IP address or hostname • <IP> – Specifies the RADIUS server's IP address • <HOSTNAME> – Specifies the RADIUS server's hostname
<WORD>	Specify the RADIUS server's shared secret.
<USERNAME>	Specify username for authentication.
<PASSWORD>	Specify the password.
wlan <WLAN-NAME> ssid <SSID>	Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. • ssid <SSID> – Specify the WLAN SSID.
on <DEVICE-NAME>	Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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. • test – Tests the RADIUS server's account with user provided parameters
[<IP>|<HOSTNAME>]	Sets the IP address or hostname of the RADIUS server • <IP> – Specify the RADIUS server's IP address. • <HOSTNAME> – Specify the RADIUS server's hostname.
<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> ssid <SSID>	Optional. Tests the RADIUS server on the local WLAN. Specify the local WLAN name. • ssid <SSID> – Specify WLAN SSID.
on <DEVICE-NAME>	Optional. This is a recursive parameter also applicable to the WLAN parameter. Performs tests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • full – Performs a full configuration validation • partial – Performs a partial configuration validation
on <DEVICE-NAME>	Optional. Performs full or partial configuration validation on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 *Organizationally Unique Identifier* (OUI) part of the MAC address • <OUI/MAC> – Specify the MAC address or its OUI. The first six digits of the MAC address is the OUI. Use the AABBCC or AA-BB-CC format to provide the OUI.
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: • on <DEVICE-NAME> – Optional. Displays information for a specified device. If no device is specified, the system displays information for logged device(s) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <WLAN-NAME> – Specify the WLAN name.
status detail	Displays only failed IP ACL to WLAN mappings • details – Optional. Displays all (failed as well as successful) IP ACL to WLAN mapping status
on <DEVICE-OR-DOMAIN-NAME>	Optional. Specifies the device name or the RF Domain name. • <DEVICE-OR-DOMAIN-NAME> – 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.

```
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>	Optional. Displays DHCP lease information for a specified router interface • <INTERFACE> – Specify the router interface name.
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>	Optional. Displays DHCP lease information for a VLAN interface • <1-4094> – Specify a VLAN index from 1 - 4094.
wwan1	Optional. Displays DHCP lease information for a Wireless WAN interface
on <DEVICE-NAME>	The following keywords are common to all of the above: • on <DEVICE-NAME> – Optional. Displays DHCP lease information for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 *file descriptors* (fds) opened by key processes, such as the CFGD. When executed, the command displays only the file name and FD.
pkts	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 `service > start-shell` 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 diag on page 980 (profile config mode). 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 `service > clear > diag > pkts` command. Following are the loop codes and the corresponding loop reasons: • (5) - "pkt looping in dataplane" • (51) - "loop in packet path" • (367) - "wispe encapsulation loop" • (432) - "mcx loop prevention" • (532) - "Port loop detected" • (536) - "packet loop detected by wireless bridge" • (41) - "IPv4 TTL exceeded" • (493) - "IPv6 TTL exceeded" • (540) - "mint TTL exceeded"

```
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>	Optional. Displays diagnostic statistics for a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service show guest-registration [export-status|import-status|restore-status]
```

show	Displays running system statistics based on the parameters passed
guest-registration	Displays status of the guest-registration database snapshot related processes (export, import, and restore) Note: To export, import, or restore a guest-registration database, use the `service > guest-registration > [backup|export|import]` command.]

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. • <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 *Forwarding Information Base* (FIB)
fib6	Displays FIB IPv6 static routing entries 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 • <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 • 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. • <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 *Process Monitor* (PM) 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. • <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: 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: Optional. Displays diagnostics statistics on a specified device or domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 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. • <DEVICE-NAME> – Specify the name of the service platform.

```
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: • If a radar has been discovered by the AP • The time of discovery
vlan-usage	Displays VLAN statistics across WLANs
on <DEVICE-NAME>	The following keywords are common to all of the above: • on <DEVICE-NAME> – Optional. Displays running system statistics on a specified device. If no device is specified, the system displays information for the logged device. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • proc – Displays dataplane proc entries based on the parameter selected Note: These proc entries provide statistics on each wireless client on the WLAN. Note: For the meshpoint parameter, it displays proc entries about neighbors.
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. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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: • radio1 – Selects radio 1 • radio2 – Selects radio 2.
<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. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 • <DOMAIN-NAME> – Specify the RF Domain name.

```
service snmp sysoid wing5
```

service snmp sysoid wing5	Configures a new *sysObjectID* (sysoid), in the MIB, for devices running WiNG 5.X devices 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 RFS 4000 using the WiNG 4.X image differs from another RFS 4000 running the WiNG 5.X image. This command is applicable only to RFS 4000 platform, since it has the same sysoid supported in WiNG 4.X and WiNG 5.X. The WiNG 4.X sysoids are: • RFS 4000 – 1.3.6.1.4.1.388.18 The WiNG 5.X sysoids are: • RFS 4000 – 1.3.6.1.4.1.388.50.1.1.35

```
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	Sends a test message to the syslog server to confirm server availability
	
	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.
	• <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). This is the default setting.

on <DEVICE-NAME>	Optional. Executes the command on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service ssm trace pattern <WORD> {on <DOMAIN-NAME>}
```

ssm trace	Displays the SSM module trace based on parameters passed
pattern <WORD>	Configures the pattern to match • <WORD> – Specify the pattern to match.
on <DEVICE-NAME>	Optional. Displays the SSM module trace on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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]	Specifies the beacon measurement mode. The following modes are available: • Active – Requests beacon measurements in the active mode • Passive – Requests beacon measurements in the passive mode • Table – Requests beacon measurements in the table mode
ssid [<SSID>|any]	Specifies if the measurements have to be made for a specified SSID or for any SSID • <SSID> – Requests beacon measurement for a specified SSID • any – Requests beacon measurement for any SSID

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. • <CHANNEL-LIST> – Request includes a list of channels. The client has to send beacon measurements only for those channels included in the request. • none – Request applies to all channels
on <DEVICE-NAME>	Optional. Sends requests on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service wireless client quiet-element [start|stop]
```

wireless client trigger-bss-transition	Enables the quite-element information in beacons sent to wireless clients
start	Enables the quite-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 quite-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. • <0-65535> – Specify a time from 0 -65535 seconds.
url <URL>	Specifies session termination URL
on <DEVICE-OR-DOMAIN-NAME>	Optional. Sends request on a specified device • <DEVICE-OR_DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • deauth-imminent – Sends a de-authentication imminent frame • subscription-remediation – Sends a subscription remediation needed frame
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 • <DEVICE-NAME> – Specify the name of the device (AP, wireless controller, or service platform)
<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 *Traffic Identifier* (TID) • <0-7> – Select the TID from 0 - 7.

```
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 • <WORD> – Specify the pattern to match.
on <DEVICE-NAME>	Optional. Displays the wireless module trace on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <DOMAIN-NAME> – Specify the name of the RF Domain.

```
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 • all – Removes all clients from the blacklist • mac <MAC> – Removes a specified client form the blacklist • <MAC> – Specify the wireless client's MAC address.

```
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 • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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 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|force-configured-state]
service database replica-set add member [<IP>|<FQDN>] [arbiter|priority <0-255>]
service database replica-set delete member [<IP>|<FQDN>]
service database replica-set force-configured-state
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 <1-1000000>,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 <1-1000000>,
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: • usbX:/path/file
<URL>	Specify the location URL of the file to be copied. Both IPv4 andIPv6 address formats are supported. • tftp://<hostname|IPv4/IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]>/path/file

```
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 • global – Copies extensive statistical data of all configured RF Domains • rf-domain <DOMAIN-NAME> – Copies extensive statistical data of a specified RF Domain. Specify the domain name.
<FILE>	Specify the location to copy file using the following format: • usbX:/path/file
<URL>	Specify the location URL of the file to be copied. Both IPv4 andIPv6 address formats are supported. • tftp://<hostname|IPv4/IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]>/path/file

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service database authentication create-user username <USER-NAME> password <PASSWORD>
```

database	Performs database related actions Note: This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.
authentication create-user username <USER-NAME> password <PASSWORD>	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 database on page 66 (user exec mode). • username <USER-NAME> – Configures database username • password <PASSWORD> – Configures a password for the username specified above 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 database-policy global config on page 299 and database-client-policy global-config on page 296.

```
service database authentication delete-user username <USER-NAME>
```

database	Performs database related actions Note: 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 • username <USER-NAME> – Deletes the username identified by the <USER-NAME> keyword Once deleted, the database cannot be accessed using the specified combination of username and password.

```
service database compact [all|captive-portal|nsight]
```

database	Performs database related actions Note: This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.
compact [all| captive-portal| nsight]	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. • all – Compacts collections within all databases (captive-portal and NSight) being maintained • captive-portal – Compacts all collections within the captive portal database only • nsight – Compacts all collections within the NSight database only

```
service database [maintenance-mode|primary-stepdown|remove-all-files|start-shell]
```

database	Performs database related actions Note: 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 database-policy (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 Note: 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 database-policy (global config mode) .

add member [<IP>|<FQDN>]	Adds members to the database replica set • <IP> – Identifies the member by its IP address. Specify the member's IP address. • <FQDN> – Identifies the member by its FQDN. Specify the member's FQDN address. Note: Ensure that the identified members have the database instance running prior to being added to the replica set.
[arbiter| priority <0-255>]	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. • 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. • priority <0-255> – Identifies the new member as not being the arbiter and configures its priority value. • <0-255> – Specify the priority value from 0 - 255. Not applicable for the arbiter. 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.

```
service database replica-set delete member [<IP>|<FQDN>]
```

database	Performs database related actions Note: This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.
replica-set	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 database-policy (global config mode) .
delete member [<IP>|<FQDN>]	Deletes members from an existing database replica set • <IP> – Identifies the member by its IP address. Specify the member's IP address. • <FQDN> – Identifies the member by its FQDN. Specify the member's FQDN address.

```
service database replica-set force-configured-start
```

database	Performs database related actions **Note:** This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.
replica-set	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 database-policy (global config mode) .
force-configured-start	Forces the replica-set to move to the configured state

```
service database server [restart|start|stop]
```

database	Performs database related actions **Note:** This command is supported only on the NX 95XX, NX 96XX, and VX 9000 platforms.
server [restart|start|stop]	Performs the following actions on the database server: • restart – Restarts the server • start – Starts the server • stop – Stops the server

```
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 *MiNT Link Control Protocol* (MLCP) links • lsp-db – Clears MiNT Label *Switched Path* (LSP) database • mlcp – Clears MLCP links
debug-log [flash-and-syslog| flash-only]	Enables debug message logging • flash-and-syslog – Logs debug messages to the flash and syslog files • flash-only – Logs debug messages to the flash file only
expire [lsp|spf]	Forces expiration of LSP and recalculation of *Shortest Path First* (SPF) • lsp – Forces expiration of LSP • spf – Forces recalculation of SPF
flood [csnp|lsp]	Floods control packets • csnp – Floods our *Complete Sequence Number Packets* (CSNP) • lsp – Floods our LSP

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • on – Defines the packet capture location
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 *Radio Interface Module* (RIM)
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|radio|src| tcp|udp| vlan|wlan]	Optional. Filters packets based on the option selected (must be used as a last option). The filter options are: • <LINE> – Defines user defined packet capture filter • arp – Matches ARP packets • capwap – Matches CAPWAP packets • cdp – Matches CDP packets • dot11 – Matches 802.11 packets • dropreason – Matches packet drop reason • dst – Matches IP destination • ether – Matches Ethernet packets • failed – Matches failed 802.11 transmitted frames • host – Matches host destination • icmp – Matches ICMP packets • icmp6 – Matches ICMPv6 frames • ip – Matches IPV4 packets • ipv6 – Matches IPV6 packets • l2 – Matches L2 header • l3 – Matches L3 header • l4 – Matches L4 header • mint – Matches MiNT packets • lldp – Matches LLDP packets • net – Matches IP in subnet • not – Filters out any packet that matches the filter criteria (For example, if not TCP is used, all tcp packets are filtered out) • port – Matches TCP or UDP port • priority – Matches packet priority • radio – Matches radio • rssi – Matches Received Signal Strength Indication (RSSI) of received radio signals • src – Matches IP source • stp – Matches STP packets • tcp – Matches TCP packets • tcp6 – Matches TCP over IPv6 packets • udp – Matches UDP packets • udp6 – Matches UDP over IPv6 packets • vlan – Matches VLAN • wlan – Matches WLAN
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
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	Captures packets to a specified file. Provide the file name and location in the following format: FILE – flash:/path/file • flash:/path/file • usbX:/path/file URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported. • nvram:startup-config • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>@<hostname|IP>[:port]>/path/file • tzsp – *Tazman Sniffer Protocol* (TZSP) host. Specify the TZSP host's IP address or 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>])}
```

pktcap on radio	Captures data packets on a radio (802.11)
<1-1024>	Captures data packets on a specified radio • <1-1024> – specify the radio index from 1 - 1024.
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>	Optional. Sets a specified number of packets to capture • <1-1000000> – 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>	Optional. Filters packets based on the option selected (must be used as a last option) • <LINE> – Define a packet capture filter or select any one of the available options.
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
tcpdump	Optional. Decodes the TCP dump

verbose	Optional. Displays full packet body
write	Captures packets to a specified file. Provide the file name and location in the following format: • flash:/path/file • usbX:/path/file URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported. • nvram:startup-config • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>@<hostname|IP>[:port]>/path/file • tzsp – TZSP host. Specify the TZSP host's IP address or hostname.

```
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	Captures data packets at a specified interface • on – Specify the capture location.
interface [<INTERFACE>| ge <1-4>| me1| port-channel <1-2>| vlan <1-4094>]	Captures packets at a specified interface. The options are: • <INTERFACE> – Specify the interface name. • ge <1-4> – Selects a GigabitEthernet interface index from 1 - 4 • me1 – Selects the FastEthernet interface • port-channel <1-2> – Selects a port-channel interface index from 1- 2 • vlan <1-4094> – Selects a VLAN ID from 1 - 4094
acl-name <ACL>	Optional. Specify the ACL that matches the ACL name for the 'deny' location
count <1-1000000>	Optional. Sets a specified number of packets to capture • <1-1000000> – 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>	Optional. Filters packets based on the option selected (must be used as a last option) • <LINE> – Define a packet capture filter or select any one of the available options.
hex	Optional. Provides binary output of the captured packets
rate <1-100>	Optional. Specifies the packet capture rate • <1-100> – Specify a value from 1 - 100 seconds.
snap <1-2048>	Optional. Captures the data length • <1-2048> – Specify a value from 1 - 2048 characters.
tcpdump	Optional. Decodes the TCP dump

verbose	Optional. Displays full packet body
write	Captures packets to a specified file. Provide the file name and location in the following format: • flash:/path/file • usbX:/path/file URL – Specify the location URL to capture file. Both IPv4 and IPv6 address formats are supported. • nvram:startup-config • tftp://<hostname|IP>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file • sftp://<user>@<hostname|IP>[:port]>/path/file • tzsp – TZSP host. Specify the TZSP host's IP address or hostname.

```
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	Sends a signal to a process • tech-support – Copies extensive system information useful for troubleshooting
abort	Sends an abort signal to a process, and forces it to dump to core • <PROCESS-NAME> – Specify the process name.
kill	Sends a kill signal to a process, and forces it to terminate without a core • <PROCESS-NAME> – Specify the process name.

```
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: **Note:** 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: • usb1:/path/file • usb2:/path/file
<URL>	Specify the location URL to copy file. Both IPv4 and IPv6 formats are supported. • tftp://<hostname|IPv4/IPv6>[:port]/path/file • ftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]/path/file • sftp://<user>:<passwd>@<hostname|IPv4/IPv6>[:port]>/path/file

Usage Guidelines

The NX 95XX service platforms 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 • <10-300> – Specify a value from 10 - 300. The default is 200.
upgrade-history <10-100>	Sets the size of the upgrade history file • <10-100> – Specify a value from 10 - 100. The default is 50.
reboot-history <10-100>	Sets the size of the reboot history file • <10-100> – Specify a value from 10 - 100. The default is 50.
virtual-machine-history <10-200>	Sets the size of the virtual-machine history file • <10-200> – Specify a value from 10 - 200. The default is 100. This command is applicable only to the NX 95XX and NX 96XX series service platforms. Use the `no > service > set > virtual-machine-history > {on <DEVICE-NAME>}` command to revert the history file size to 100.
on <DEVICE-NAME>	Optional. Sets the size of history files on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
service show cli
```

show cli	Displays running system configuration details • cli – Displays the CLI tree of the current mode

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#
```

```
ap505-13403B*#service show crash-info
-------------------------------------------------------------------------------
                  CRASH FILE                     SIZE         LAST MODIFIED
-------------------------------------------------------------------------------
  panic_201902201741_AP505_7.1.0.0-075D.tar.gz   18727   Wed Feb 20 17:41:07 2019
-------------------------------------------------------------------------------
ap505-13403B*#
```

```
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 NX 9500 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 zl mesh_root on ROOT1-ap81xx-71174C
       | SUBZONE
       | 0    1    2    3    4    5    6    7
-------+-----------------------------------------
  ZONE |
       | GEN  TX   RX   BEA  TXF
 2-LLC | 0    0    0    0    0
       | GEN  TX   RX   NBR  LQM  LSA
 3-ND  | 0    0    0    0    0    0
       | GEN
 4-ORL | 0
       | GEN  TX   RX   HEL  PRO
 5-LQ  | 0    0    0    0    0
       | GEN
 6-PS  | 0
       | GEN  ROOT NBR  REC
 7-RS  | 0    0    0    0
       | GEN
 8-IA  | 0
       | GEN  SET  GET
11-MGT | 0    0    0
       | GEN  RX   TX   R0   LMST LSUP LKEY KEY
13-LSA | 0    0    0    0    0    0    0    0
       | GEN  SCAN TRIG
```

```
14-ACS | 0    0    0
       | GEN
15-EAP | 0
       | GEN
16-L2P | 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 zl 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 zl mesh_root on ROOT1-ap81xx-71174C
       | SUBZONE
       | 0    1    2    3    4    5    6    7
-------+-----------------------------------------
  ZONE |
       | GEN  TX   RX   BEA  TXF
 2-LLC | 0    0    0    0    0
       | GEN  TX   RX   NBR  LQM  LSA
 3-ND  | 0    0    7(D) 0    0    0
       | GEN
 4-ORL | 0
       | GEN  TX   RX   HEL  PRO
 5-LQ  | 0    0    0    0    0
       | GEN
 6-PS  | 0
       | GEN  ROOT NBR  REC
 7-RS  | 0    0    0    0
       | GEN
 8-IA  | 0
       | GEN  SET  GET
11-MGT | 0    0    0
       | GEN  RX   TX   R0   LMST LSUP LKEY KEY
13-LSA | 0    0    0    0    0    0    0    0
       | GEN  SCAN TRIG
14-ACS | 0    0    0
       | GEN
15-EAP | 0
       | GEN
16-L2P | 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 zl 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 zl mesh_root on ROOT1-ap81xx-71174C 5

ROOT1-ap81xx-71174C#service wireless meshpoint zl mesh_root on ROOT1-ap81xx-71174C
       | SUBZONE
       | 0    1    2    3    4    5    6    7
-------+-----------------------------------------
  ZONE |
       | GEN  TX   RX   BEA  TXF
 2-LLC | 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-autorized-keys "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDPERY9aTibRYlFMnERTYP2iyylJ00YElxjUElY7Zm9Ky2yeSmg15UKerJ
+IP161Gdm0AoEfXyeheRntK
+Z6NWHa341RWJ0UrQMcp7hSEE5jbDpLKJOuEoW22Ag45BZzMV7EnM7lHowboNsQhSzX5uBBlVViWlBxBqDroX4BcuB
/CFugezHTt95UQ2ZRUfHvePS6jQdOArf1alwk0Slcsz4HNSl5KDutJ4VY+6vRvlf5Gy/
3GNehMwNsmsRKK4UVKV5RpuuKIjkbZE+goPFAKYVPNmZngjaOyDfvNGE7JIwmYlti/
AId6tv2zAbM4qSomWAgUOO0hkXS9m4m74FnHPr extreme@extreme-quadcore"
Successfully added the ssh key
rfs4000-1BE644#

rfs4000-1BE644#no service load-ssh-autorized-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: ge1, 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: ge1, 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: ge1, 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: ap7161-99BB7C - 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 on page 677.

write

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
write [memory|terminal]
```

Parameters

```
write [memory|terminal]
```

memory	Writes to the *non-volatile* (NV) memory
terminal	Writes to the terminal

Examples

```
nx9500-6C8809>write memory
[OK]
nx9500-6C8809>
```

7 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 33: Show Commands

Command	Description
show on page 680	Displays settings for the specified system component
adoption on page 686	Displays adoption related information
bluetooth on page 689	Displays Bluetooth radio statistics for RF Domain member access points
boot on page 691	Displays a device's boot configuration
bonjour on page 692	Displays the configured Bonjour services available on local and remote sites
captive-portal on page 693	Displays WLAN hotspot functions
captive-portal-page-upload (show commands) on page 694	Displays captive portal Web pages upload related information
cdp on page 696	Displays a CDP *(Cisco Discovery Protocol)* neighbor table
classify-url on page 697	Queries a specified global data center or a pre-configured classification server for the category of a specified URL.
clock on page 697	Displays the system clock
cluster on page 698	Displays device-cluster related statistics
cmp-factory-certs on page 699	Displays factory installed CMP certificates
commands on page 700	Displays command list
context on page 700	Displays information about the current context

Table 33: Show Commands (continued)

Command	Description
critical-resources on page 701	Displays critical resources deployed within the managed network and associated statistics
crypto on page 702	Displays encryption mode information
database on page 705	Displays database-related statistics and status
device-upgrade on page 706	Displays device firmware upgradation information for devices adopted by a wireless controller or access point
dot1x on page 708	Displays dot1x information on interfaces
dpi on page 710	Displays statistics for all configured and canned applications
environmental-sensor on page 714	Displays environmental sensor's historical data (applicable only to AP 8132)
event-history on page 716	Displays event history
event-system-policy on page 717	Displays event system policy configuration information
ex3500 on page 718	Displays EX3500-related statistical data
extdev on page 720	Displays external device (T5 or EX3500) configuration error history
fabric-attach on page 721	Displays the current status of VLAN to I-SID assignments for all ports
file on page 722	Displays file system information
file-sync on page 723	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
firewall on page 725	Displays wireless firewall information
global on page 729	Displays global information for network devices based on the parameters passed
gps (show command) on page 730	Displays the geographical coordinates (latitude and longitude) of the device for which the GPS coordinates search process has been triggered
gre on page 731	Displays GRE tunnel related information
guest-registration on page 732	Displays guest registration statistics based on the option and time entered
interface on page 740	Displays interface status
iot-device-type-imagotag on page 743	Displays the configuration of ESL communicator on a specified AP or on all APs within an RF Domain.
ip on page 744	DisplaysIP related information
ip-access-list-stats on page 751	Displays IP access list statistics
ipv6 on page 752	Displays IPv6 related information
ipv6-access-list on page 756	Displays IPv6 access list statistics
l2tpv3 on page 756	Displays L2TPv3 *(Layer 2 Tunnel Protocol Version 3)* information
lacp on page 759	Displays LACP *(Link Aggregation Control Protocol)* related information
ldap-agent on page 762	Displays an LDAP agent's join status (join status to a LDAP server domain)

Table 33: Show Commands (continued)

Command	Description
licenses on page 762	Displays installed licenses and usage information
lldp on page 764	Displays LLDP *(Link Layer Discovery Protocol)* information
logging on page 765	Displays logging information
mac-access-list-stats on page 766	Displays MAC access list statistics
mac-address-table on page 767	Displays MAC address table entries
macauth on page 768	Displays details of wired ports that have MAC address-based authentication enabled
mac-auth-clients on page 770	Displays MAC-authenticated clients based on the parameters passed
mint on page 771	Displays MiNT protocol configuration commands
ntp on page 774	Displays NTP server related information
password-encryption on page 775	Displays password encryption status
pppoe-client on page 775	Displays PPPoE *(Point to Point Protocol over Ethernet)* client information
privilege on page 776	Displays current privilege level information
radius on page 777	Displays the amount of access time consumed and the access time remaining for all guest users configured on a RADIUS server
reload on page 779	Displays scheduled reload information
rf-domain-manager on page 779	Displays RF Domain manager selection details
role on page 780	Displays role-based firewall information
route-maps on page 781	Display route map statistics
rtls on page 781	Displays RTLS *(Real Time Location Service)* statistics of access points
running-config on page 782	Displays configuration file contents
session-changes on page 790	Displays configuration changes made in the current session
session-config on page 791	Displays configurations made in the current session
sessions on page 792	Displays a list of currently active open sessions on the device
site-config-diff on page 792	Displays the difference between site configuration available on NOC and the actual site configuration
smart-rf on page 793	Displays Smart RF management statistics
snmpv3 (show command) on page 798	Displays the SNMPv3 Engine ID
spanning-tree on page 799	Displays spanning tree information
startup-config on page 801	Displays complete startup configuration script on the console
t5 on page 802	Displays adopted T5 controller details. This command is applicable only on the RFS 4000, NX 95XX, NX 96XX, and VX 9000.
terminal on page 810	Displays terminal configuration parameters
timezone on page 810	Displays timezone information for the system and managed devices
traffic-shape on page 810	Displays traffic-shaping related configuration details and statistics

Table 33: Show Commands (continued)

Command	Description
tron (show command) on page 812	Displays the TRON-capable and TRON-enabled WiNG AP's operating configuration.
upgrade-status on page 813	Displays image upgrade status
version on page 814	Displays a device's software and hardware version
vrrp on page 815	Displays VRRP details
virtual-machine on page 816	Displays the VM *(virtual-machine)* configuration, logs, and statistics
web-filter on page 844	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.
what on page 846	Displays details of a specified search phrase
wireless on page 819	Displays wireless configuration parameters
wwan on page 847	Displays the wireless WAN status

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
  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
  gps                           GPS commands
  gre                           Show l2gre tunnel info
  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
  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
  snmpv3                        Snmpv3
  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
  tron                          TRON functions
  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)#
```

```
nx9500-6C8809(config)#show clock
2017-04-06 15:49:10 IST
nx9500-6C8809(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
  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
gps                             GPS commands
gre                             Show l2gre tunnel info
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
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
snmpv3                          Snmpv3
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
tron                            TRON functions
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#

nx9500-6C8809#show adoption offline
-------------------------------------------------------------------------------------------
------
MAC                 HOST-NAME     TYPE    RF-DOMAIN   TIME OFFLINE  CONNECTED-TO  LAST-
KNOWN-IP
-------------------------------------------------------------------------------------------
------
74-67-F7-5C-63-F0  ap8432-5C63F0  ap8432   default      unknown        None
unknown
74-67-F7-07-02-35  ap8432-070235  ap8432   default      unknown        None
unknown
-------------------------------------------------------------------------------------------
------
Total number of devices displayed: 2
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
  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
  gps                         GPS commands
  gre                         Show l2gre tunnel info
  guest-registration          Guest registration commands
  interface                   Interface Configuration/Statistics commands
  iot-device-type-imagotag    Iot device type imagotag
  ip                          Internet Protocol (IP)
  ipv6                        Internet Protocol version 6 (IPv6)
```

```
  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
  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
  snmpv3                        Snmpv3
  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
  tron                          TRON functions
  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.

Use this command to view details of devices adopted by the logged device.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show adoption [config-errors|controllers|history|info|log|offline|pending|status|timeline]
show adoption offline {all|on <DEVICE-NAME>}
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 status of offline devices (unadopted devices) Note: The `show → adoption → offline` command displays the following information regarding offline (unadopted) devices: MAC Address, Host-Name, Type, RF-Domain, Time Offline, Connected-To, and Last-Know-IP.

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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>}	Displays adoption logs, for the specified device. If no device name is specified, the system displays logs for the logged device. • adoptee – Displays adoption logs for adoptee devices (APs, wireless controllers, and service platforms). To view logs for a specific 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. `2013-01-19 22:00:13:MLCP_TAG_CLUSTER_MASTER not present and this device is a controller. Ignoring` • on <DEVICE-NAME> – Optional. Displays adoptee status and details for the device identified by the <DEVICE-NAME> keyword <DEVICE-NAME> – Specify the device's name. • 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. • <MAC> – 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 <MAC> keyword. on <DEVICE-NAME> – Optional. Displays adopter status and details for the device identified by the <DEVICE-NAME> keyword. Specify the adopter device's name. <DEVICE-NAME> – Specify the adopter device's name. Note: 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.

`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 {include-ipv6}	Displays information about adopted controllers. This is applicable in a Hierarchically managed network, where site controllers are adopted by the NOC controllers. • include-ipv6 – Optional. Displays the controller's IPv6 address, if assigned, in the output
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 {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 logged device. • summary – Optional. Displays a summary of all devices or specific adopted by the logged device. Note: The `show → adoption → status` command displays the following adopted device status information: Device Name, Version, CFG-Stat, Msgs, Adopted-By, Last-adoption, Up-Time, and IP-Address.
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: • on <DEVICE-NAME> – Optional. Displays a device's adoption information, based on the parameter passed. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx9500-6C8809#show adoption status
-------------------------------------------------------------------------------------------------
----------------
DEVICE-NAME   VERSION      CFG-STAT  MSGS  ADOPTED-BY    LAST-ADOPTION
UPTIME         IPv4-ADDRESS
-------------------------------------------------------------------------------------------------
----------------
ap505-134038 7.2.0.0-009D configured   No nx9500-6C8809  0 days 23:20:52  33 days
01:41:56 10.234.160.36
-------------------------------------------------------------------------------------------------
----------------
Total number of devices displayed: 1
nx9500-6C8809#

nx9500-6C8809#show adoption log adoptee on ap505-134038
2019-07-01 14:23:27:Received OK from cfgd, adoption complete to 19.6C.88.09
2019-07-01 14:23:27:Waiting for cfgd OK, adopter should be 19.6C.88.09
2019-07-01 14:23:27:Adoption state change: 'Connecting to adopter' to 'Waiting for
Adoption OK'
2019-07-01 14:23:27:Adoption state change: 'No adopters found' to 'Connecting to adopter'
2019-07-01 14:23:27:Try to adopt to 19.6C.88.09 (cluster master 19.6C.88.09 in adopters)
2019-07-01 14:23:24:MLCP created VLAN link on VLAN 1, offer from B4-C7-99-6C-88-09
2019-07-01 14:23:24:MLCP VLAN link already exists
2019-07-01 14:23:24:Sending MLCP Request to B4-C7-99-6C-88-09 vlan 1
2019-07-01 14:20:04:Adoption state change: 'Waiting to retry' to 'No adopters found'
2019-07-01 14:19:59:cfgd notified dpd2 of unadoption, restart adoption after 5 seconds
2019-07-01 14:19:59:Adoption state change: 'Adopted' to 'Waiting to retry'
2019-07-01 14:19:59:Adopter 19.6C.88.09 is no longer reachable, cfgd notified
2019-07-01 14:19:59:All adopters lost, restarting MLCP
2019-07-01 14:19:54:MLCP link vlan-1 offerer 19.6C.88.09 lost, restarting discovery
2019-06-28 12:45:05:Received OK from cfgd, adoption complete to 19.6C.88.09
2019-06-28 12:45:05:Waiting for cfgd OK, adopter should be 19.6C.88.09
--More--
nx9500-6C8809#

nx9500-6C8809(config-device-94-9B-2C-13-40-38)#show adoption history
-------------------------------------------------------------------------
          MAC         TYPE   EVENT       TIME-STAMP         REASON
```

```
-------------------------------------------------------------------------
  94-9B-2C-13-40-38  ap505  adopted   2019-07-01 14:23:27     N.A.
-------------------------------------------------------------------------
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#
```

bluetooth

Displays Bluetooth radio statistics for RF Domain member access points. The AP-8432 and AP-8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. Both these model access points support the *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.

The 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 *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.

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>	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. • <DEVICE-NAME> <1-1> – Optional. Specify the access point's hostname or MAC address. • <1-1> – 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 The following information is displayed: • access point's hostname as its network identifier • access point's alias. If an alias has been defined for the access point its listed here. The alias value is expressed in the form of *<hostname>:B<Bluetooth_radio_number>*. If the access point has a administrator assigned hostname, it is used in place of the access point's default hostname. • access point's factory encoded MAC address • access point and bluetooth radio's administrator assigned area of deployment (the AP's geographical location) • bluetooth radio's state (on/off) • bluetooth radio's reason for inactivity (in case the radio is off) • bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network • bluetooth radio's functional mode: bt-sensor or le-beacon • bluetooth radio's beacon period • bluetooth radio's beacon type • descriptive text on any error that's preventing the Bluetooth radio from operating
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. • <BT-RADIO-MAC> – Specify the Bluetooth radio's MAC address. The system only displays statistics related to the specified Bluetooth radio.
on <DEVICE-OR-DOMAIN-NAME>	The following keywords are recursive and common to all of the above. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays Bluetooth radio statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – 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. If no device/RF Domain is specified, the results include data for all Bluetooth radios within the controller's RF Domain. 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.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: Use the *on <DEVICE-NAME>* option to view a remote device's boot configuration.

Examples

```
ap510-133B38#show boot
------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
------------------------------------------------------------------------------
  Primary       06/28/2019 02:43:33     07/02/2019 13:28:20     7.2.0.0-009D
  Secondary     06/21/2019 02:34:38     06/25/2019 14:46:00     7.2.0.0-006D
------------------------------------------------------------------------------
Current Boot       : Secondary
Next Boot          : Primary
```

```
Software Fallback  : Enabled
ap510-133B38#
nx9500-6C8809>show boot
-------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
-------------------------------------------------------------------------------
  Primary       06/28/2019 09:31:40     07/01/2019 13:57:47     7.2.0.0-009D
  Secondary     06/26/2019 09:37:54     06/28/2019 12:38:00     7.2.0.0-008D
-------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
nx9500-6C8809>
```

bonjour

Displays the configured Bonjour services available on local and remote sites

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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
-------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
nx9500-6C8809#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
filter	This parameter is recursive and can be used with any of the above parameters to define additional filters. Optional. Defines additional filters. Use one of the following options: **captive-portal**, **ip**, **ipv6**, **state**, **vlan**, or **wlan**.
captive-portal [<CAPTIVE-PORTAL>| not <CAPTIVE-PORTAL>]	Optional. Displays captive portal client and client session information, based on the captive portal name passed • <CAPTIVE-PORTAL> – Specify the captive portal name. Displays client details for the specified captive portal. • not <CAPTIVE-PORTAL> – Inverts the match selection. Displays client details for all captive portals other than the specified captive portal.
ip [<IPv4>|not <IPv4>]	Optional. Displays captive portal client/client sessions information, based on the IPv4 address passed • <IPv4> – Specify the client's IPv4 address. Displays information of the client identified by the <IPv4> parameter. • not <IPv4> – Inverts the match selection. Displays client details for all clients other than the one identified by the <IPv4> parameter.

ipv6 [<IPv6>|not <IPv6>]	This filter option is available only for the 'include-ipv6' keyword. Optional. Displays captive portal client/client sessions information, based on the IPv6 address passed • <IPv6> – Specify the client's IPv6 address. Displays information of the client identified by the <IPv6> parameter • not <IPv6> – Inverts the match selection. Displays client details for all clients other than the one identified by the <IPv6> parameter.

state [pending| success| not [pending|success]]	Optional. Filters clients/client sessions based on the client's authentication state
	• pending – Displays information of clients redirected for authentication
	• success – Displays information of successfully authenticated clients
	• not [pending|success] – Inverts match selection
	  • pending – Displays information of successfully authenticated clients (opposite of pending authentication)
	  • success – Displays information of clients redirected for authentication (opposite of successful authentication)

vlan [<VLAN-ID>| not <VLAN-ID>]	Optional. Displays captive portal client/client sessions information based on the VLAN ID passed • <VLAN-ID> – Specify the VLAN ID. Displays client details for the specified VLAN. • not <VLAN-ID> – Inverts match selection. Displays client details for all VLANs other than the one identified by the <VLAN-ID> parameter.
wlan [<WLAN-NAME>| not <WLAN-NAME>]	Optional. Displays captive portal client/client sessions information based on the WLAN name passed • <WLAN-NAME> – Specify the WLAN name. Displays client details for the specified WLAN. • not <WLAN-NAME> – Inverts match selection. Displays client details for all WLANs other than the one identified by the <WLAN-NAME> parameter.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload history within a specified RF Domain. Specify the RF Domain name.

```
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 • on <RF-DOMAIN-NAME> – Optional. Displays captive portal page upload status within a specified RF Domain. Specify the RF Domain name. • on <RF-DOMAIN-MANAGER> – Optional. Displays captive portal page upload status for a specified RF Domain Manager. Specify the RF Domain Manager name.

```
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) • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.

Examples

```
nx7500-7F2C13#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#
```

cdp

Displays the CDP neighbor table

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • on <DEVICE-NAME> – Optional. Displays table details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
on <DEVICE-NAME>	Optional. Displays table details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <URL-TO-QUERY> – Specify the URL to query.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Optional. Specify the controller or access point name. If the device name is not specified, the system displays all cluster history.
members {detail}	Displays cluster members configured on the logged device • detail – Optional. Displays detailed information of known cluster members
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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show commands
```

Parameters

```
None
```

Examples

```
v(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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • include-factory – Optional. Includes factory defaults

Examples

```
nx9500-6C8809>show context
!
! Configuration of NX9500 version 7.1.0.0-010D
!
!
version 2.6
!
!
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"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 tra--More--
nx9500-6C8809>
```

critical-resources

Displays critical resource information. Critical resources are resources vital to the network.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 status	Displays current status of in-progress *certificate management protocol* (CMP) requests For more information, see Crypto-CMP Policy on page 1846.

```
show crypto ike sa {detail|peer <IP>} {on <DEVICE-NAME>}
```

crypto ike sa	Displays *Internet Key Exchange* (IKE) SA *(security association)* statistics
detail	Displays detailed IKE SA statistics

peer <IP>	Optional. Displays IKE SA statistics for a specified peer • <IP> – Specify the peer's IP address in the A.B.C.D format
on <DEVICE-NAME>	Optional. Displays IKE SA statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • 1 – Displays IKEv1 statistics • 2 – Displays IKEv2 statistics
peer <IP>	Optional. Displays IKE SA version statistics for a specified peer • <IP> – Specify the peer's IP address in the A.B.C.D format
on <DEVICE-NAME>	The following keyword is recursive and common to the 'peer ip' parameter: • on <DEVICE-NAME> – Optional. Displays IKE SA statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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

crypto ipsec sa	Displays *Internet Protocol Security* (IPSec) SA statistics. The IPSec encryption authenticates and encrypts each IP packet in a communication session
detail	Optional. Displays detailed IPSec SA statistics
on <DEVICE-NAME>	Optional. Displays IPSec SAs on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show crypto ipsec 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 • <IP> – Specify the peer's IP address in the A.B.C.D format. • detail – Displays detailed IPSec SA statistics for the specified peer
on <DEVICE-NAME>	The following keyword is recursive: • on <DEVICE-NAME> – Optional. Displays IPSec SAs on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 *Privacy-Enhanced Mail* (PEM) format
on <DEVICE-NAME>	The following keyword is recursive: • on <DEVICE-NAME> – Optional. Displays public key on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {(on <DEVICE-NAME>)}
```

crypto pki	Displays PKI related information
trustpoints	Displays WLAN trustpoints 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: • on <DEVICE-NAME> – Optional. Displays trustpoints configured on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx9500-6C8809(config)#show crypto key rsa public-key-detail

RSA key name: ting        Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtLj11yR38+/mcInGRlrw
3DaasuTJhKsWg7kcSVkM7RLd/Wq/mPZEsqwFLnvFIm4rVIke+mVdWBqV4oGE1TUm
Z4YqKtzlANSAG7EZREr3MXEIHd49NHYeK8U+1EAmHN9F21XCxTO+yRMngKDJeHfz
Za2/64PdBsnRlV4nqCGMGHbbaaCwGe5X0a

RSA key name: default_rsa_key        Key-length: 2048
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3hyJDk9aMk97X3PhoyMb
6nufFLFUkpF9YwSqO2fNyp9SutqpoML/VAMHHotmaa6SsxPURF8mC66bT7De32r7
wwPd7pIWwALTscwCzd3CrB1jY8s2OQ7ZHGCH6MLau+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, NX 96XX, 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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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/
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/
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/SMSMlH6sPITMGTLMu6wRYFEUgKgO01Wn/BohE
5n+uuhY0xiZQsN0LS7IaA8Yb9rX859YRQ7v9By5aEpi1NIDR4KX09Xs3TqIB+5v2
jE3vv7OsKK+LX63bCIoYo35MX251T2pHdL+fMdLfKPMt8ZbzYzx2b22Yvukfg0gm
xHsMCB+bLAsfkjeCPgHCAq/WWi3Kxna6ysFjp8J4US2Bm+GL1COvALbCQBwkPPN+
o7M90qT40AubibBkeID2S9rkQkKcXqGESbL5xG6ip+26jIxiLv7GP6/SQZGFOqC/
ZZEkCNhGhkiyktiOIxBfoXwoy66sqQ4KBwLF449eqBe7Svel/dzpFPNfYZpW8SMY
LD6iLTPR9BddjsBBej8kGGc5R+M0R6lgQFEew2WX6Rqz45YTGEcfOkl8c9wl3taD
xn4imhI/esjMppFDu5muxRHF5RHa5RncTGnsMfc7ndvUl78QaGHLZvDqjNLBUnuP
c8QmyohEnKf70TYx/ruG9Vb2AP0Jw5OODTNh2lmaoFjicKYQr+xIHUJpHc0qY43C
5WzlWf84CK67cu7kOPiJoaxvufzSXhJB18BiCXTuv40+ZZ6e3PcisZuIrPXxCZup
GJ3KpuHq61IJyVCydFd5zl4Fho+RGaQ9dlDIlaLjbW+YT4CEH1bTiUmreUt+D/X2
zcB9nec77wIIAcdfl2qysgGIqmkI3jRI89d3XM5Y7Kc2TuXBVZOazYldPj+qE/yi
EgVWcbtvyS834jit35MGbVXhvQ2d45qgo42WZwdTVLXC9memzoKa3YIZoj32uP3U
iOrzD8E1gMte4gDE/KmGkYya+hsWswBmKC1v0gj5NQ6TejYS4z+nefqLHUSVXbQ8
NxRel1huGi8P1ns4dWCwClWp8GpxUTa7GuN1DySA7/l2OJM=

nx9500-6C8809#
```

device-upgrade

Displays firmware upgradation information for devices adopted by a wireless controller or access point

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <DOMAIN-NAME>}	Displays firmware upgrade history • on <DOMAIN-NAME> – Optional. Displays upgrade history for all devices within a specified RF Domain. Specify the RF Domain name.

load-image-status	Displays firmware image loading status. The output displays the <DEVICE> image loading status in percentage.
	For example,
	`#show device-upgrade load-image-status`
	`Download of ap81xx firmware file is 47 percent complete`

versions {on <DEVICE-OR-DOMAIN-NAME>}	Displays firmware image versions • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays firmware image versions loaded on specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the AP, wireless controller, service platform, or RF Domain name.

```
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>| 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. • <DOMAIN-NAME> – Specify the RF Domain name. • rf-domain-manager – Select to view devices upgraded by the RF Domain manager.
summary {on <DOMAIN-NAME>}	Displays a summary of in-progress upgrade processes • on <DOMAIN-NAME> – Optional. Displays in-progress upgrade processes within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

Examples

```
nx9500-6C8809#show adoption status
-------------------------------------------------------------------------------------------------
---------------------------------------
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-
ADOPTION                  UPTIME     IPv4-ADDRESS
-------------------------------------------------------------------------------------------------
---------------------------------------
ap505-134038      7.1.2.0-011D    version-mismatch No   nx9500-6C8809       0 days
00:01:40    46 days 02:05:56    10.234.160.36
-------------------------------------------------------------------------------------------------
---------------------------------------
Total number of devices displayed: 4
nx9500-6C8809#

nx9500-6C8809#device-upgrade ap505-134038
-------------------------------------------------------------------------------
         CONTROLLER             STATUS                   MESSAGE
-------------------------------------------------------------------------------
  B4-C7-99-6C-88-09         Success         Queued 1 devices to upgrade
-------------------------------------------------------------------------------
nx9500-6C8809#

nx9500-6C8809#show device-upgrade status
Number of devices currently being upgraded : 0
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 ERROR   UPGRADED BY
-------------------------------------------------------------------------------------------------
ap505-13403  wait for reboot  immediate  immediate   0        0       -      nx9500-6C8809
-------------------------------------------------------------------------------------------------
nx9500-6C8809#

nx9500-6C8809#show device-upgrade history on default
-------------------------------------------------------------------------------------
    Device      RESULT        TIME        RETRIES     UPGRADED-BY  LAST-UPDATE-ERROR
-------------------------------------------------------------------------------------

  ap505-134038   done  2019-05-27 17:23:53    0      nx9500-6C8809         -

  ap505-134038   done  2019-04-11 15:15:17    0      nx9500-6C8809         -

  ap505-134038   done  2019-03-21 14:30:46    0      nx9500-6C8809         -
--More--
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 – AP 6522, AP 6562, AP 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP-8163, AP-8432, AP-8533
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX

Note

Dot.1x authenticator configuration is supported on the following platforms:

- Access Points – AP 6522, AP 7161, AP 7161, AP 7502, AP-8163
- Wireless Controllers – RFS 4000
- Service Platforms – NX 5500, NX 75XX

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • on <DEVICE-NAME> – Optional. Displays dot1x information for all interfaces on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
dot1x {on <DEVICE-NAME>}	Optional. Displays dot1x information for interfaces on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

```
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 • <1-4> – Select the interface index from 1 - 4.

port-channel <1-2>	Displays dot1x for a specified port channel interface • <1-2> – Select the interface index from 1 - 2.
on <DEVICE-NAME>	The following keywords are common to all of the above parameters: • on <DEVICE-NAME> – Optional. Displays dot1x interface information on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

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 *Deep Packet Inspection* (DPI) 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 983 (profile config mode).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show dpi [app|per-purview-category|purview-app-category|purview-application|
purview-application-policy]
show dpi app [stats|wireless-clients|wlan]
show dpi app stats [<APPLICATION-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}
show dpi app wireless-clients stats <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
show dpi app wlan stats [<WLAN-NAME>|all] on <RF-DOMAIN-NAME>
show dpi per-purview-category stats <PURVIEW-APP-CATEGORY-NAME>
[bytes-in|bytes-out|total-bytes] {on <DEVICE-OR-DOMAIN-NAME>}
show dpi purview-application brief
show dpi purview-application-policy stats <PURVIEW-APP-POLICY-NAME>
{on <DEVICE-NAME>}
```

Parameters

```
show dpi app wireless-clients stats <MAC> {<DEVICE-OR-DOMAIN-NAME>}
```

dpi app wireless-clients <MAC>	Displays application-usage statistics for all wireless clients or a specified wireless client • <MAC> – Displays application usage stats for a specified wireless client. To view applications used by a specific wireless client, specify the client's MAC address. **Note:** If no MAC address is specified, application usage stats is displayed for all wireless clients within the network (i.e., all RF Domains)
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays application-usage stats for wireless clients associated with a specified device or within a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the access point, wireless controller, service platform, or RF Domain. **Note:** If you specify an access point name, the application usage stats for wireless clients associated with the specified AP is displayed. In case of an RF Domain, application usage stats for all wireless clients associated with APs within the specified RF Domain is displayed.

```
show dpi app stats [<APPLICATION-NAME>|all] {on <DEVICE-OR-DOMAIN-NAME>}
```

dpi app stats	Displays statistics for an application or application category • app – Displays statistics for a specified application or all applications Note: The applications are the RF Domain member allowed applications whose data (bytes) are passing through the WiNG 7.X.X managed network.
[<APPLICATION-NAME>|all]	This parameter is common to the 'app' and 'app-category' keywords. • <APPLICATION-NAME> – Displays statistics for a specified application • all – Displays statistics for all applications
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.

```
show dpi app wlan stats [<WLAN-NAME>|all] on <RF-DOMAIN-NAME>
```

dpi app wlan stats [<WLAN-NAME>|all]	Displays application-usage statistics for all wireless clients associating with a specified network or all networks • <WLAN-NAME> – Displays application usage stats for a specified wireless network. • all - Displays application usage stats for all wireless networks configured within the system.
on <RF-DOMAIN-NAME>	Optional. Displays application-usage stats for wireless clients within a specified RF Domain • <RF-DOMAIN-NAME> – Specify the name of the RF Domain.

```
show dpi purview-application-policy stats <PURVIEW-APP-POLICY-NAME>
{on <DEVICE-NAME>}
```

dpi purview-application-policy stats	Displays statistics for an existing Purview application policy
<PURVIEW-APP-POLICY-NAME>	Displays statistics for a specified Purview application-policy. Specify the policy name.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays Purview application-policy related 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.

```
show dpi purview-application brief
```

dpi purview-application brief	Displays a brief summary of purview-applications their status and configuration

```
show dpi per-purview-category stats <PURVIEW-APP-CATEGORY-NAME>
[bytes-in|bytes-out|total-bytes] {on <DEVICE-OR-DOMAIN-NAME>}
```

dpi per-purview-category stats	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.
<PURVIEW-APP-CATEGORY-NAME>	Specify the Purview application category name. The system displays statistics for the top ten applications in this category.

[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

```
ap560-135433#show dpi app stats all
-------------------------------------------------------------------------------------
APPLICATION          BYTES_UPLOADED        BYTES_DOWNLOADED       NUM_FLOWS
-------------------------------------------------------------------------------------
SSDP                    864                    0                     1
LLMNR                   396                    0                     10
Google                  91.253 KB              306.998 KB            20
Taboola                 8.516 KB               30.384 KB             1
AppNexus                1.087 KB               3.394 KB              1
Yahoo_Ads               7.753 KB               33.404 KB             5
Google_Ads              30.101 KB              30.914 KB             3
ndtv-custom             16.754 KB              164.662 KB            2
Encrypted_Web           12.610 KB              367.589 KB            1
Google_Analytics        11.473 KB              38.588 KB             4
-------------------------------------------------------------------------------------
ap560-135433#

ap560-135433#show dpi app wireless-client stats
========== Wireless Client 60-67-20-A8-26-28 Application Statistics ==========
-------------------------------------------------------------------------------
       APPLICATION          BYTES_UPLOADED    BYTES_DOWNLOADED     NUM_FLOWS
-------------------------------------------------------------------------------
  Unknown                  139.050 KB        999.103 KB          79
  AddThis                  0                 0                   521
  Adobe_Ads                0                 0                   6
  Aggregate_Knowledge      0                 0                   4
-------------------------------------------------------------------------------
ap560-135433#

ap560-135433#show dpi app wlan stats 560-libdpi on remote
========== Wlan 560-libdpi Application Statistics ==========
-------------------------------------------------------------------------------
          APPLICATION       BYTES_UPLOADED          BYTES_DOWNLOADED
-------------------------------------------------------------------------------
  AddThis                       0                       0
  Adobe_Ads                     0                       0
  Aggregate_Knowledge           0                       0
  Akamai                        0                       0
  Amazon_Web_Services           0                       0
  Aol_Advertising               0                       0
  AppNexus                      0                       0
```

```
--------------------------------------------------------------------------------
ap560-135433#
```

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 senor 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     Light       Humidity
                                           (deg. C)      (lux)         (%)
                                       ----------- 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Examples

```
nx9500-6C8809#show event-history
Generated on '2017-09-21 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 75XX, NX 95XX, NX 96XX

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 **Note:** 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 • <DEVICE-NAME> – Specify the device's 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>}
```

ex3500 interfaces counters	Displays EX3500 interface counters based on the option selected. The options are: **ether-like**, **ethernet**, **ext-if-table**, **if-table**, **portUtil**, **rmon**
ether-like stats	Displays *Managed Information Base* (MIB) 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 • <1-1> – Specify the EX3500 unit's identifier from 1 - 1. • <1-52> – Specify the port number from 1 - 52. This range varies for the EX3524 (1-28) and EX3548 (1-52) devices. Note: 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 *remote monitoring* (RMon) statistics
on <EX3500-DEVICE-NAME>	Optional. Executes the command on a specified EX3500 device • <DEVICE-NAME> – Specify the device's name.

```
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 • <DEVICE-NAME> – Specify the device's name.

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, NX 96XX

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 series service platform.
on <T5/EX3500-DEVICE-NAME>	Optional. Displays configuration error history on a specified T5 or EX3500 device • <T5/EX3500-DEVICE-NAME> – Specify the name of the device.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • active – If the VLAN to I-SID mapping is accepted by the FA Server and applied to the VLAN traffic from the client. • pending – If the VLAN to I-SID mapping acceptance is not achieved (i.e, pending acceptance)
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. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Example

The Following example shows the fabric-attach VLAN to ISID assignment configured on the ap510-13403B access point:

```
nx9600-7F3B2C#
ap510 94-9B-2C-13-40-38
 use profile default-ap510
 use rf-domain default
 hostname ap510-13403B
 interface ge1
  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 ap505-13403B

 Assignment status for port : ge1
 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show file [information <FILE>|systems]
```

Parameters

```
show file [information <FILE>|systems]
```

information <FILE>	Displays file information • <FILE> – Specify the file name.
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  nvram:
            84            81     2   flash  flash:
           137            82    40       -  vmsdb:
ap8432-070235#
```

```
nx9500-6C8809#show file information startup-config
nvram: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:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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	Displays the following file-synchronization configuration details: • automatic file-syncing enabled or disabled. The default setting is disabled. 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 `file-sync > auto` command. For more information, see file-sync on page 995 (profile config mode). • Number of access points to which the certificate can be simultaneously uploaded. The default is 10. To modify the number of simultaneous uploads, in the controller's device/profile configuration mode, execute the `file-sync > count <1-20>` command. For more information, see file-sync on page 995 (profile config mode). • Scheduled certificate upload, if any, details, such time and date of upload. To schedule certificate upload, use the `file-sync > wireless-certificate` command. For more information, see file-sync on page 995 (profile config mode).
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 file-sync on page 995 (profile config mode).
status	Displays status of the file synchronization between the controller and its adopted access point.
on <DEVICE-OR-DOMAIN- NAME>	Optional. Displays file synchronization settings and status on a specified device or RF Domain • <DEVICE-OR-DOMAIN- NAME> – Specify the name of the controller, service platform, or RF Domain.

Examples

```
nx9500-6C8809#show file-sync configuration
File Sync Configuration Information
  Auto                          : Disabled
  Simultaneous Upload Count     : 128
```

```
  Wireless Bridge Cert Load Time : Thu Jan 29 23:23:35 2019
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
-------------------------------------------------------------------------------------
AP510-491220   done    2019-05-29 01:37:32  0    B4-C7-99-6C-88-09       -
nx9500-6C8809#
ap505-13403B#show file-sync configuration
File Sync Configuration Information
  Auto                          : Disabled
  Simultaneous Upload Count     : 10
ap505-13403B#
```

firewall

Displays wireless firewall information, such as *Dynamic Host Configuration Protocol* (DHCP) 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}	Displays DHCP snoop table entries • snoop-table – Displays DHCP snoop table entries 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.
on <DEVICE-NAME>	The following keyword is common to the 'DHCP snoop table' and 'DoS stats' parameters: • on <DEVICE-NAME> – Optional. Displays snoop table entries, or DoS stats on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • wired-wired – Wired to wired flows • wired-wireless – Wired to wireless flows • wireless-wired – Wireless to wired flows • wireless-wireless – Wireless to wireless flows
dst port <1-65535>	Optional. Matches the destination port with the specified port • port <1-65535> – Specifies the destination port number from 1 - 65535
ether [dst <MAC>| host <MAC>| src <MAC>| vlan <1-4094>]	Optional. Displays Ethernet filter options • dst <MAC> – Matches only the destination MAC address • host <MAC> – Matches flows containing the specified MAC address • src <MAC> – Matches only the source MAC address • vlan <1-4094> – Matches the VLAN number of the traffic with the specified value. Specify a value from 1- 4094.
flow-type [bridged|natted|routed| wired|wireless]	Optional. Matches the traffic flow type • bridged – Bridged flows • natted – Natted flows • routed – Routed flows • wired – Flows belonging to wired hosts • wireless – Flows containing a mobile unit
icmp {code|type}	Optional. Matches flows with the specified *Internet Control Message Protocol* (ICMP) version 4 code and type • code – Matches flows with the specified ICMPv4 code • type – Matches flows with the specified ICMPv4 type
icmpv6 {code|type}	Optional. Matches flows with the specified ICMP version 6 code and type • code – Optional. Matches flows with the specified ICMPv6 code • type – Optional. Matches flows with the specified ICMPv6 type
igmp	Optional. Matches *Internet Group Management Protocol* (IGMP) flows

ip [dst <IP>| host <IP>| proto <0-254>| src <IP>]	Optional. Filters firewall flows based on the IPv4 parameters passed • dst <IP> – Matches destination IP address • host <IP> – Matches flows containing IPv4 address • proto <0-254> – Matches the IPv4 protocol number with the specified number • src <IPv4> – Matches source IP address
ipv6 [dst <IPv6>| host <IPv6>| proto <0-254>| src <IPv6>]	Optional. Filters firewall flows based on the IPv6 parameters passed • dst <IPv6> – Matches destination IPv6 address • host <IPv6> – Matches flows containing IPv6 address • proto <0-254> – Matches the IPv6 protocol number with the specified number • src <IPv6> – Matches source IPv6 address
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 • on <DEVICE-NAME> – Optional. Displays firewall flows on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
stats {on <DEVICE-NAME>}	Optional. Displays active session summary • on <DEVICE-NAME> – Optional. Displays active session summary on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

wireless-client <MAC>	Optional. Displays wireless clients firewall flows • <MAC> – Specify the MAC address of the wireless client.
on <DEVICE-NAME>	Optional. Displays all firewall flows on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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-advt                       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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **offline**, **online**, and **rf-domain**.
filter{offline|online}	Optional. Specifies additional filters • offline – Optional. Displays global information for offline devices only • online – Optional. Displays global information for online devices only

```
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: **offline**, **online**, and **rf-domain**.

filter rf-domain [<DOMAIN-NAME>| not <DOMAIN-NAME>]	Optional. Specifies additional filters
	• rf-domain – Optional. Displays global information for all devices in a specified RF Domain
	  • <DOMAIN-NAME> – Optional. Displays information for all devices within the domain identified by the <DOMAIN-NAME> keyword
	  • not <DOMAIN-NAME> – Optional. Displays information for all devices in domains not matching the <DOMAIN-NAME> keyword

```
show global domain managers
```

global domain managers	Displays global information for all RF Domains managers in the network.

Examples

```
vnx9500-6C8809(config)#show global device-list filter rf-domain TechPubs
-------------------------------------------------------------------------------------------------
--------------------
           MAC      HOST-NAME       TYPE          CLUSTER        RF-DOMAIN        ADOPTED-
BY     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
-------------------------------------------------------------------------------------------------
-----------
                    RF-DOMAIN                                MANAGER          HOST-NAME
APS  CLIENTS
-------------------------------------------------------------------------------------------------
-----------
                        default   ? rf-domain manager 00-15-70-38-03-E7 not in
configuration
                       TechPubs                    00-15-70-81-74-2D
rfs6000-81742D    0        0
-------------------------------------------------------------------------------------------------
-----------
Total number of RF-domain displayed: 2
nx9500-6C8809(config)#
```

gps (show command)

Displays the geographical coordinates (latitude and longitude) of the device for which the GPS coordinates search process has been triggered. The system displays the last recorded GPS coordinates of the device.

This feature is supported only on AP7662, which has a built-in, GPS hardware that starts and stops the GPS coordinates search process. To view the GPS coordinates of an AP7622, initiate GPS coordinates search and then execute the 'show > gps' command.

Note

For more information on starting and stopping the GPS coordinate search process, see #unique_622.

Supported in the following platforms:

- AP 7622

Syntax

```
show gps coordinates {on <DEVICE-NAME>}
```

Parameters

```
show gps coordinates {on <DEVICE-NAME>}
```

show gps coordinates	Displays the GPS coordinates of a device Note: The command displays the last recorded GPS coordinates of the device.
on <DEVICE-NAME>	Optional. Specifies the name of the AP whose GPS coordinates are to be displayed. Use this option if executing the command on the controller or virtual controller to which the AP is adopted. Note: If you do not specify a device name, the system initiates the search on the logged device. And if the logged device is not an AP7662 model access point, an error message returns. If

Examples

```
ap7662-8BDE4D#show gps coordinates
GPS Search is in progress.
Last location recorded at UTC time : Mon Apr 23 22:10:54 2018 :  Latitude : 13.036N
Longitude : 77.3827E
ap7662-8BDE4D#
```

gre

Displays layer 2 *Generic Routing Encapsulation* (GRE) 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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the access point, controller, or service platform.

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 75XX, 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. Note: Use the `service > guest-registration > backup [delete|restore]` command to delete these snapshots and to restore deleted snapshots. For more information, see service on page 623 (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 *operating system* (OS) 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: • 1-Day – Displays previous day's statistics • 1-Month – Displays previous month's statistics • 1-Week – Displays previous week's statistics • 2-Hours – Displays last 2 hours statistics • 30-Mins – Displays last 30 minutes statistics • 5-Hours – Displays last 5 hours statistics • all – Displays statistics from the day the database was created

[rfdomain <DOMAIN-NAME| wlan <WLAN-NAME>]	Use the following options as additional filters:
	• rfdomain <DOMAIN-NAME> – Optional. Displays guest registration statistics for a specified RF Domain.
	  • <DOMAIN-NAME> – Specify the RF Domain name.
	• wlan <WLAN-NAME> – Optional. Displays guest registration statistics for a specified WLAN.
	  • <WLAN-NAME> – Specify the WLAN name.

```
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 • <EMAIL-ADDRESS> – Specify the client's e-mail address.
mac <MAC>	Displays statistical data for the client with MAC address matching the <MAC> parameter • <MAC> – Specify the client's MAC address
member <MEMBER-ID>	Displays statistical data for the client with member ID matching the <MEMBER-ID> parameter • <MEMBER-ID> – Specify the client's member ID.
mobile <MOBILE-NUMBER>	Displays statistical data for the client with mobile number matching the <MOBILE-NUMBER> parameter • <MOBILE-NUMBER> – Specify the client's mobile number.
name <NAME>	Displays statistical data for the client with name matching the <NAME> parameter • <MOBILE-NUMBER> – Specify the client's 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>)}
```

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 • 1-Day – Displays previous day's statistics • 1-Month – Displays previous month's statistics • 1-Week – Displays previous week's statistics • 2-Hours – Displays last 2 hours statistics • 30-Mins – Displays last 30 minutes statistics • 5-Hours – Displays last 5 hours statistics • all – Displays statistics from the day the database was created

[rfdomain <DOMAIN-NAME| wlan <WLAN-NAME>]	Use the following options as additional filters:
	• rfdomain <DOMAIN-NAME> – Optional. Displays guest registration statistics for a specified RF Domain.
	  • <DOMAIN-NAME> – Specify the RF Domain name.
	• wlan <WLAN-NAME> – Optional. Displays guest registration statistics for a specified WLAN.
	  • <WLAN-NAME> – Specify the 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>}
```

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. 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 report-royalty-application on page 245 (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 • 1-Day – Displays previous day's captive portal clients' Loyalty Application analytics • 1-Month – Displays previous month's captive portal clients' Loyalty Application analytics • 1-Week – Displays previous week's captive portal clients' Loyalty Application analytics • 2-Hours – Displays last 2 hours captive portal clients' Loyalty Application analytics • 30-Mins – Displays last 30 minutes captive portal clients' Loyalty Application analytics • 5-Hours – Displays last 5 hours captive portal clients' Loyalty Application analytics • all – Displays the entire Loyalty Application analytics, from the day the database was created

{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
	• rfdomain <RF-DOMAIN-NAME> – Displays Loyalty App analytics for a specified RF Domain
	  • <RF-DOMAIN-NAME> – Specify the RF Domain name.
	• wlan <WLAN-NAME> – Displays Loyalty App analytics for a specified WLAN
	  • <WLAN-NAME> – Specify the WLAN name.

```
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: • 1-Day – Displays previous day's statistics • 1-Month – Displays previous month's statistics • 1-Week – Displays previous week's statistics • 2-Hours – Displays last 2 hours statistics • 30-Mins – Displays last 30 minutes statistics • 5-Hours – Displays last 5 hours statistics • all – Displays statistics from the day the database was created
facebook	Displays guest users using Facebook to log in
rfdomain <DOMAIN-NAME>	Displays guest users for a specific RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

wlan <WLAN-NAME>	Displays guest users for a specific WLAN • <WLAN-NAME> – Specify the WLAN name.
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 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-4> – Select the Gigabit Ethernet interface index from 1 - 4.
me1	Optional. Displays Fast Ethernet interface status and configuration
port-channel <1-2>	Optional. Displays port channel interface status and configuration • <1-2> – Specify the port channel index from 1 - 2.
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 • <1-4094> – Specify the *Switch Virtual Interface* (SVI) VLAN ID from 1 - 4094.
wwan1	Optional. Displays Wireless WAN interface status, configuration, and counters
on <DEVICE-NAME>	The following keywords are common to all of the above interfaces: • on <DEVICE-NAME> – Optional. Displays interface related information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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            MAC           RX-PKTS     RX-BYTES     RX-DROP     TX-PKTS     TX-
BYTES       TX-DROP
-------------------------------------------------------------------------------------------------
--------------------
 vlan1      B4-C7-99-6C-88-09   2571193     341672167    0           625888
90924957     0
 ge1        00-1E-67-4B-BF-BC   2326629     348759017    0           1080855
244588229    0
 ge2        00-1E-67-4B-BF-BD   0           0            0           0
0            0
 port..nel1 00-1E-67-4B-BF-BC   2326631     348759243    0           1080857
244588673    0
-------------------------------------------------------------------------------------------------
--------------------
nx9500-6C8809(config)#
```

The following command shows the state of Energy-efficient Ethernet, where:

- **`Enable`**: Indicates if Energy-Efficient Ethernet is *enabled* or *disabled* on the selected physical port. A value of '1' indicates enabled and '0' indicates disabled.
- **`Active`**: Indictaes if Energy-Efficient Ethernet is *active* or *inactive* on the selected physical port. A value of '1' indicates EEE is active and '0' indicates inactive. Note, will be active only if the devices on both ends of the phhysical link support EEE.

```
ap505-13403B#show interface ge 1
Interface ge2 is UP
  Hardware-type: ethernet, Mode: Layer 2, Address: 94-9B-2C-13-40-39
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 1G, Maximum 2.5G
  Duplex: Admin Auto, Operational Full
  EEE: Enable 1, Active 1
  Active-medium: n/a
  Switchport settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0
    Received 0 unicasts, 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 0, bytes 0, dropped 0
    Sent 0 unicasts, 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

ap505-13403B#
```

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
on <DEVICE-NAME>	Optional. Displays configuration on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP or RF Domain.

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     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     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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *Address Resolution Protocol* (ARP) 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: • on <DEVICE-NAME> – Optional. Displays ARP configuration details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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. This command is applicable to the RFS 4000, NX 95XX, and NX 96XX 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: • 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) • local-as – Filters routes carrying the local-as attribute (these routes are not sent outside the local AS) • no-advertise – Filters routes carrying the no-advertise attribute (these routes are not advertised to any peers) • no-export – Filters routes carrying no-export attribute (these routes are not exported to next AS)
community-list	Optional. Displays routes that are members of communities included in the specified BGP community-list • <1-500> – Specify the community-list number. • <WORD> – Specify the community-list name.
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: • advertised-routes – Displays route information for routes advertised to the selected neighbor device • received-routes – Displays route information for routes received from the selected neighbor device • routes – Displays the route information for routes learned from the selected neighbor device If no neighbor IP address is specified, the system displays all neighbor-related routes on the logged device.
on <DEVICE-NAME>	Optional. Displays BGP routing table statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
paths	Optional. Displays BGP path details
prefix-list <PREFIX-LIST-NAME>	Optional. Displays routes confirming to the specified prefix-list • <PREFIX-LIST-NAME> – Specify the prefix list name.

regexp <LINE>	Optional. Displays routes matching the specified AS path regular expression • <LINE> – Specify the regular expression.
route-map <ROUTE-MAP-NAME>	Optional. Displays routes matching the specified route map • <ROUTE-MAP-NAME> – Specify the route map name.

```
show ip ddns bindings {on <DEVICE-NAME>}
```

ip ddns	Displays *Dynamic Domain Name Server* (DDNS) configuration details
bindings {on <DEVICE-NAME>}	Displays DDNS address bindings • on <DEVICE-NAME> – Optional. Displays address bindings on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • on <DEVICE-NAME> – Optional. Displays server status and network details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • on <DEVICE-NAME> – Optional. Displays DHCP address bindings on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show ip extcommunity-list [<1-500>|<NAME>]
```

ip extcommunity-list [<1-500>| <NAME>]	Displays the specified extended community list details • <1-500> – Specify the extended community number from 1 - 500. • <NAME> – Specify the extended community name. This command is applicable to the RFS 4000, NX 95XX, and NX 96XX model devices.

```
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: • on <DEVICE-NAME> – Optional. Displays IP related information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <1-4095> – Specify the VLAN ID from 1 - 4095. • on <DEVICE-NAME> – Optional. Displays the IGMP snooping mrouter configuration on a specified device <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <1-4095> – Specify the VLAN ID from 1 - 4095.
<IP>	Optional. Specifies the multicast group IP address
on <DEVICE-NAME>	The following keyword is recursive and common to the 'ip' parameter: • on <DEVICE-NAME> – Optional. Displays configuration details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • on <DEVICE-NAME> – Optional. Displays interface status and summary, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show ip nat translations verbose {on <DEVICE-NAME>}
```

ip nat translations	Displays *Network Address Translation* (NAT) translations
verbose	Displays detailed NAT translations • on <DEVICE-NAME> – Optional.Displays NAT translations on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • C – Connected • G – Gateway • O – OSPF route • S – Static route Note: Flags 'S' and 'O' identify static learned routes and dynamic learned routes respectively.
<INTERFACE-NAME>	Optional. Displays route table details for a specified interface. Specify the interface name
ge <1-4>	Displays GigabitEthernet interface route table details • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
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: • on <DEVICE-NAME> – Displays route table details, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • on <DEVICE-NAME> – Optional. Displays specified device details • vlan <1-4094> – Displays VLAN interface details • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.
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: • on <DEVICE-NAME> – Optional. Displays overall OSPF information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 ingore-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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Displays all or a specified IP access list statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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:

```
nx9500-6C8809(config)#ip access-list auto-tunnel-acl
nx9500-6C8809(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
nx9500-6C8809(config-ip-acl-auto-tunnel-acl)#
```

The following example dispalys the statistics for the 'auto-tunnel-acl' ACL:

```
nx9500-6C8809#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

nx9500-6C8809#
```

ipv6

Displays IPv6 related information and statistical data

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>|ppppoe1|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. • on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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. • on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • <IF-NAME> – Optional. Specify the interface name. • brief – Optional. Displays a brief summary of IPv6 status and configuration on the specified interface
on <DEVICE-NAME>	This parameter is common to all of the above keywords. • on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 *Multicast Listener Discovery Protocol* (MLD) 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. • on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show ipv6 route {<IF-NAME>|ge <1-X>|me1|port-channel <1-2>|ppppoe1|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. • on <DEVICE-NAME> – Optional. Displays the specified information on a device (access point, wireless controller, or service platform) • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 session information

Note
This command is not available in the USER EXEC mode.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show l2tpv3 {on|statistics|tunnel|tunnel-summary}
show l2tpv3 {on <DEVICE-NAME>}
show l2tpv3 statistics {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>}	Displays L2TPv3 tunnel and session details or summary • on <DEVICE-NAME> – Optional. Displays L2TPv3 information on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

```
show l2tpv3 statistics {on <DEVICE-NAME>)}
```

show l2tpv3 statistics	Displays L2TPv3 Tunnel and session statistics. It displays the information, such as the number of packets transmitted and received, the rate of transmission, number of packets dropped, etc.
on <DEVICE-NAME>	Optional. Executes the command on a specified device • <DEVICE-NAME> - Specify the name of the access point, wireless controller, or service platform. Note: If you do not specify a device name, the system executes the command on the logged device.

```
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>	Optional. Displays a specified L2TPv3 tunnel information • <L2TPv3-TUNNEL-NAME> – Specify the L2TPv3 tunnel name.

session <L2TPv3-SESSION- NAME>	Optional. Displays a specified L2TPv3 tunnel session information • <L2TPv3-SESSION-NAME> – Specify the session name.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'session <L2TPv3-SESSION-NAME>' parameter. • on <DEVICE-NAME> – Optional. Displays a L2TPv3 tunnel and session details, based on the parameters passed, on a specified device. • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

```
show l2tpv3 {tunnel-summary} {on <DEVICE-NAME>}
```

l2tpv3	Displays L2TPv3 tunnel and session details or summary Note: For an L2TPv3 tunnel over Auto IPSec, the tunnel status is displayed as: Established (secured by ipsec)
tunnel-summary {on <DEVICE-NAME>}	Optional. Displays L2TPv3 tunnel summary • on <DEVICE-NAME> – Optional. Displays L2TPv3 tunnel summary on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

```
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>	The following keyword is common to the 'down' and 'up' parameters: • on <DEVICE-NAME> – Optional. Displays summary, for un-established or established tunnels, on a specified device • <DEVICE-NAME> – Specify the name of AP, wireless controller, or service platform.

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 *Link Aggregation Control Protocol* (LACP) related information

Note

For more information on enabling dynamic LACP, see lacp on page 1027 (profile - inf - ge - config mode), lacp-channel-group on page 1028 (profile - inf - ge - config mode), and lacp on page 1279 (device config mode).

Supported in the following platforms:

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

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 • <1-4> – Select the port-channel index number from 1 - 4. Note, LACP is supported only on the NX 5500, NX 75XX, NX 95XX, NX 96XX model service platforms. 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 • sys-id – Shows the LACP system identifier and priority. This is the identifier assigned to the LACP peers (devices).

Examples

```
NOC-controller#show interface port-channel 1
Interface port-channel1 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
pc1              xge1                   11548      12479          0          0
0          0
pc1              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 pc1 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 pc1 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <DEVICE-NAME> – Specify the name of the device running the LDAP server (access point, wireless controller, or service platform).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show licenses {borrowed|lent}
```

Parameters

```
show licenses {borrowed|lent}
```

licenses {borrowed|lent}	Displays installed licenses and usage information • borrowed – Optional. Displays information on licenses borrowed • lent – Optional. Displays information on licenses lent.

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 *Link Layer Discovery Protocol* (LLDP) related information

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • detail – Optional. Displays detailed aggregated LLDP neighbors table Note: If the 'on' keyword is used without the 'detail' keyword, the system displays LLDP neighbors table summary on the specified device or RF Domain.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'report detail' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Displays aggregated LLDP neighbors table on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

Examples

```
nx9500-6C8809#show lldp neighbors
-------------------------
Chassis ID: 00-18-71-D0-0B-00
System Name: TechPubs-ProCurve-Switch
Platform: ProCurve J8697A Switch 5406zl, revision K.12.1X, ROM K.11.03 (/sw/code/build/
btm(sw_esp1))
Capabilities: Bridge  Router
Enabled Capabilities: Bridge
Local Interface: ge1, 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show logging {on <DEVICE-NAME>}
```

Parameters

```
show logging {on <DEVICE-NAME>}
```

logging {on <DEVICE-NAME>}	Displays logging information on a specified device • <DEVICE-NAME> – Optional. Specify the name of the AP or wireless controller.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. **Note:** 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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 1197 (profile-config-mode).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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	• Displays MAC authentication related information for all interfaces

interface [<INTERFACE-NAME>| ge <1-5>| port-channel <1-3>| t1e1 <1-4>|up <1-2>| xge <1-4>]	Optional. Displays MAC authentication related information for a specified interface. Specify the interface using one of the following options: • <INTERFACE-NAME> – Selects the interface identified by the <INTERFACE-NAME> keyword • ge <1-5> – Selects the GigabitEthernet interface identified by the index number • port-channel <1-3> – Selects the port channel interface identified by the index number • t1e1 <1-4> – Selects the layer 2 interface (Ethernet port) • up <1-2> – Selects the WAN Ethernet interface identified by the index number • xge <1-4> – Selects the TenGigabitEthernet interface identified by the index number
on <DEVICE-NAME>	The following keywords are common to the 'all' and 'interface' parameters: • on <DEVICE-NAME> – Optional. Displays MAC authentication related information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: 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.

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:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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: • <INF-NAME> – Optional. Displays MAC authenticated clients for the interface identified by the <INF-NAME> keyword. Specify the layer 2 (ethernet port) interface name. • ge <1-X> – 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. • port-channel <1-2> – Optional. Displays MAC authenticated clients for the selected port channel interface. Specify the port channel interface index from 1 - 2. • xge <1-4> – Optional. Displays MAC authenticated clients for the selected TenGigabitEthernet interface. Specify the interface index from 1 - 4.
on <DEVICE-NAME>	Optional. Displays MAC authenticated clients for the specified interface on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Displays MiNT protocol details on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show mint [dis|links|neighbors|tunnel-controller] {details} {(on <DEVICE-NAME>)}
```

mint	Displays MiNT protocol information based on the parameters passed
dis	Displays MiNT network *Designated Intermediate Systems* (DISes) and *Ethernet Virtualization Interconnects* (EVISes)
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>)}	The following keywords are common to the 'dis', 'links', 'neighbors', and 'tunnel-controller' parameters: • details – Optional. Displays detailed MiNT information • on <DEVICE-NAME> – Optional. This is a recursive parameter, which displays MiNT information on a specified device <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show mint lsp
```

mint	Displays MiNT protocol information based on the parameters passed
lsp	Displays this router's MiNT *Label Switched Paths* (LSPs)

```
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 • <MINT_ADDRESS> – Specify the MiNT address in the AA.BB.CC.DD format.
on <DEVICE-NAME>	The following keyword is recursive and common to the 'details' parameter: • on <DEVICE-NAME> – Optional. Displays MiNT LSP database entries on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
show mint mlcp {history} {(on <DEVICE-NAME>)}
```

mint	Displays MiNT protocol information based on the parameters passed This command displays the 'hello-interval' and 'hold-time' default values for both IP and VLAN links.
mlcp	Displays *MiNT Link Creation Protocol* (MLCP) status
history	Optional. Displays MLCP client history
on <DEVICE-NAME>	The following keyword is recursive and common to the 'history' parameter: • on <DEVICE-NAME> – Optional. Displays MLCP client history on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
NOC-NX9500#show mint stats
2 Level-1 neighbors
Level-1 LSP DB size 5 LSPs (1 KB)
Last Level-1 SPFs 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 SPFs 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#
```

ntp

Displays *Network Time Protocol* (NTP) information. NTP enables clock synchronization within a network.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show ntp [associations|status]
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]
```

Parameters

```
show ntp [associations {detail|on}|status {on <DEVICE-NAME>}]
```

ntp associations {detail|on}	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: • peer associations - where a controller or service platform synchronizes to another system or allows another system to synchronize to it, or • - server associations - where only the controller or service platform synchronizes to the SNTP resource, not the other way around. Specify the following parameters to view NTP association details: • detail – Optional. Displays detailed NTP associations • on <DEVICE-NAME> – Optional. Displays NTP associations on a specified device <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. **Note:** 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.
ntp status {on <DEVICE-NAME>}	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. • on <DEVICE-NAME> – Optional. Displays NTP association status on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform

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 (synced), # master (unsynced), + 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Displays detailed PPPoE client status or configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx9500-6C8809#show pppoe-client configuration
 PPPoE Client Configuration:
+-----------------------------------------
|  Mode          : Disabled
|  Service Name  :
|  Auth Type     : pap
|  Username      :
|  Password      : fJx5O+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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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, configured 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 on page 1584 (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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

Parameters

```
show reload {on <DEVICE-OR-DOMAIN-NAME>}
```

reload {on <DEVICE-OR-DOMAIN-NAME>}	Displays scheduled reload information for a specified device • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration on a specified device • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DEVICE-OR-DOMAIN-NAME> – specify the name of the AP, wireless controller, service platform, or RF Domain.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Displays clients associated with roles on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, and service platform.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 For more information on route maps, see route-map on page 1752.
on <DEVICE-NAME>	Optional. Displays route map statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

Examples

```
nx9500-6C8809(config)#show route-maps
nx9500-6C8809(config)#
```

rtls

Displays *Real Time Location Service* (RTLS) statistics for Access Points contributing locationing information

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show rtls [aeroscout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

Parameters

```
show rtls [aeroscout|ekahau|omnitrail] {<MAC/HOSTNAME>} {(on <DEVICE-OR-DOMAIN-NAME>)}
```

rtls	Displays Access Point RTLS statistics
aeroscout	Displays Access Point Aeroscout 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: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays Aeroscout or Ekahau statistics on a specified device or domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|nx9600|
vx9000] <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 7.1.0.0-114D`
	
	`!`
	`!`
	`version 2.6`
	`!`
	`!`
	`client-identity-group default`
	`load default-fingerprints`
	`!`
	`client-identity-group test2`
	`load default-fingerprints`
	`!`
	`===alias encrypted-string $WRITE 2 o5gA2zqj/q/REWi8rTa7vQAAAAh4yA1YNBjqTVf4mMBsGA4i`
	`!`
	`===alias encrypted-string $enAlias2 2 JI4lPuMaCdMMx7rfBeyIAwAAAAoZ6tR1FfTlFXWvSicTMVZc`
	`!`
	`--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 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. Note: If the command is executed without a keyword, the system displays the entire running configuration.
<POLICY-TYPE> <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. • <POLICY-NAME> – Specify the name of the policy (should be existing and configured).
include-factory	The following keyword is common to all policies: • include-factory – Optional. Includes factory defaults

```
show running-config {application <APPLICATION-NAME>|apllication-group <APPLICATION-GROUP-NAME>}
```

running-config	Displays current running configuration 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. Note: If the command is executed without a keyword, the system displays the entire running configuration.
application <APPLICATION-NAME>	Displays an application's configuration. The application can be system-provided or user-defined. • <APPLICATION-NAME> – Specify the application name (should be existing).
application-group <APPLICATION-GROUP-NAME>	Displays an application-group's configuration • <APPLICATION-GROUP-NAME> – Specify the application-group name (should be existing and configured).

```
show running-config {device [<MAC>|self]} {include-factory}
```

running-config	Displays current running configuration 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. Note: If the command is executed without a keyword, the system displays the entire running configuration.
device [<MAC>|self]	Optional. Displays device configuration • <MAC> – Displays a specified device configuration. Specify the MAC address of the device. • self – Displays the logged device's configuration
include-factory	This keyword is common to all of the above keywords: • include-factory – Optional. Includes factory defaults

```
show running-config {hide-encrypted-values {exclude-devices|include-factory}}
```

running-config	Displays current running configuration 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. Note: 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 `show > running-config` output • exclude-devices – Optional. Excludes devices from the running configuration displayed • include-factory – Optional. Includes factory default values in the running configuration displayed

```
show running-config {device-overrides {brief}}
```

running-config	Displays current running configuration
device-overrides brief	Optional. Displays overrides applied at the device's configuration • brief – Optional. Displays a brief summary of device overrides

```
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 • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
me1	Optional. Displays FastEthernet interface configuration
port-channel <1-2>	Optional. Displays port channel interface configuration • <1-2> – Specify the port channel interface index from 1 - 2.
pppoe1	Optional. Displays PPP over Ethernet interface configuration
vlan <1-4094>	Displays VLAN interface configuration • <1-4094> – Specify the VLAN interface number from 1 - 4094.
wwan1	Optional. Displays Wireless WAN interface configuration
include-factory	The following keyword is common to all interfaces: • include-factory - Optional. Includes factory defaults

```
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 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. Note: 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 • <IP-ACCESS-LIST-NAME> – Specify the IP access list name

<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. • <IP/IPv6/MAC-ACL-NAME> – Specify the name of the ACL (should be existing and configured).
include-factory	The following keyword is common to the 'ip-access-list' and 'mac-access-list' parameters: • include-factory - Optional. Includes factory defaults

```
show running-config {meshpoint <MESHPOINT-NAME>} {include-factory}
```

running-config	Displays current running configuration
meshpoint <MESHPOINT-NAME>	Optional. Displays meshpoint configuration • <MESHPOINT-NAME> – Specify the meshpoint name
include-factory	Optional. Includes factory defaults along with running configuration details

```
show running-config {profile [anyap|ap505|ap510|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. • <DEVICE-TYPE> – Select the device type. The options are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, and VX9000 • <PROFILE-NAME> – Specify the profile name for the selected <DEVICE-TYPE>. Note: 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 • <DOMAIN-NAME> – Displays current configuration for a specified RF Domain. Specify the RF Domain name.
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 • <WLAN-NAME> – Displays current configuration for a specified WLAN. Specify the WLAN name.
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 • <URL-FILTER-NAME> – Specify the URL filter's name.

```
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 • <URL-LIST-NAME> – Specify the URL list's name.
include-factory	Optional. Includes factory defaults

Examples

```
nx9500-6C8809#show running-config device self
!
version 2.6
!
!
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 ap505 default-ap505
profile ap505 default-ap505
 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 radio1
 interface radio2
 interface ge1
 interface ge2
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
 adoption-mode controller
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 management-policy default
management-policy default
 no telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1 1f61a6bae8aeb0f5205628a5e88a635b8f76eb11f1c44b2dcf1381a8f681f44d
role superuser access all
 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
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
nx9500-6C8809#
```

session-changes

Displays configuration changes made in the current session

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • exclude-devices – Optional. Excludes device configuration details from the output • include-factory – Optional. Includes factory defaults

Examples

```
nx9500-6C8809>show session-config
!
! Configuration of NX9500 version 7.1.0.0-010D
!
!
version 2.6
!
!
client-identity test
!
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--
nx9500-6C8809>
```

sessions

Displays CLI sessions initiated on a device

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 75XX, 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 • <SITE-NAME> – Specify the site name.

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 *Self-Monitoring At Run Time RF* (Smart 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <DOMAIN-NAME> – Specify the domain name.

```
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 Use this option to view the following: • 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. • 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. • 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. • 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.
energy	Optional. Displays AP energy for a specified AP or all APs 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 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: • <MAC> – Displays all of the above mentioned information for a specified AP, identified by its MAC address. Specify the AP's MAC address. • <DEVICE-NAME> – Displays all of the above mentioned information for a specified AP, identified by its hostname. Specify the AP's hostname.
on <DOMAIN-NAME>	Optional. Displays Access Point details on a specified RF Domain. • <DOMAIN-NAME> – Specify the domain name.

```
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. 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. 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: • on <DOMAIN-NAME> – Optional. Displays Smart RF configuration, based on the parameters passed, on a specified RF Domain • on <DOMAIN-NAME> – Specify the RF Domain name.

```
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 Specify the MAC address of the radio • <MAC> – Optional. Specify the radio's MAC address in the AA-BB-CC-DD-EE-FF format. 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.
on <DOMAIN-NAME>	The following keyword is common to all of the above parameters: • on <DOMAIN-NAME> – Optional. Displays radio details on a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
show smart-rf radio {activity|neighbors} {<MAC>|all-11an|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 • <MAC> – Specify the radio's MAC address.
all-11an	Optional. Displays radio activity of all 11a radios in the configuration
all-11bgn	Optional. Displays radio activity of all 11bg radios in the configuration
on <DOMAIN-NAME>	Optional. Displays radio activity of all radios within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 • <MAC> – Specify the Access Point's MAC address. Note: Considers all APs if this parameter is omitted
<DEVICE-NAME>	Optional. Displays interfering Access Point information on a specified device • <DEVICE-NAME> – Specify the device name. Note: Considers all APs if this parameter is omitted
on <DOMAIN-NAME>	Optional. Displays all interfering Access Point information within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 • <MAC> – Specify the Access Point's MAC address. Note: Considers all APs if this parameter is omitted
<DEVICE-NAME>	Optional. Displays all interfering neighboring Access Point information on a specified device • <DEVICE-NAME> – Specify the device name. Note: Considers all APs if this parameter is omitted
threshold <50-100>	Optional. Specifies the maximum attenuation threshold of interfering neighbors • <50-100> – Specify a value from 50 -100 dB. 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.
on <DOMAIN-NAME>	Optional. Displays radio activity of all radios within a specified RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 select-shutdown on page 1653.
<AP-MAC>	Optional. Displays if a specified AP, identified by its MAC address, was shutdown as part of the select-shutdown feature. • <AP-MAC> – Specify the access point's MAC address. **Note:** Considers all APs if this parameter is omitted.
<AP-DEVICE-NAME>	Optional. Displays if a specified AP, identified by its device name, was shutdown as part of the select-shutdown feature. • <DEVICE-NAME> – Specify the AP's device name. **Note:** Considers all APs if this parameter is omitted.
on <RF-DOMAIN-NAME>	Optional. Displays APs, within a specified RF Domain, that were shutdown as part of the select-shutdown feature. • <RF-DOMAIN-NAME> – Specify the RF Domain name.

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#
```

snmpv3 (show command)

Displays the SNMPv3 engineID

Supported in the following platforms:

- Access Points — AP 6522, AP 6562, AP 7161, AP 7502, AP 7532, AP 7562, AP 7602, AP-7612, AP 7622, AP7632, AP7662, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
show snmpv3 engineID
```

Parameters

```
show snmpv3 engineID
```

show snmpv3 engineID	displays the SNMPv3 engineID

Examples

```
NOC-NX9500>show snmpv3 engineID
SNMPv3 EngineID: 8000018480e3a66a6699599451
NOC-NX9500>
```

spanning-tree

Displays spanning tree utilization information

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *Multiple Spanning Tree* (MST) related information
configuration {on <DEVICE-NAME>}	Optional. Displays MST configuration • on <DEVICE-NAME> – Optional. Displays MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP,wireless controller, or service platform.

```
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 [<INTERFACE>| age <1-4>| me1| port-channel <1-2>| pppoe1| vlan <1-4094> wwan1]	Displays detailed MST configuration for a specified interface
	• <INTERFACE> – Displays detailed MST configuration for a specified interface. Specify the interface name.
	• age <1-4> – Displays GigabitEthernet interface MST configuration
	  • <1-4> – Select the GigabitEthernet interface index from 1 - 4.
	• me1 – Displays FastEthernet interface MST configuration
	• port-channel – Displays port channel interface MST configuration
	  • <1-2> – Select the port channel interface index from 1 - 2.
	• pppoe1 – Displays PPP over Ethernet interface MST configuration
	• vlan – Displays VLAN interface MST configuration
	  • <1-4094> – Select the SVI VLAN ID from 1 - 4094.
	• wwan1 – Displays Wireless WAN interface MST configuration

on <DEVICE-NAME>	The following keyword is common to all interfaces: Optional. Displays detailed MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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>	Optional. Displays information for a particular MST instance • <1-15> – Specify the instance ID from 1 - 15.
interface <INTERFACE-NAME>	Optional. Displays MST configuration for a specific interface instance. The options are: • <INTERFACE-NAME> – Displays MST configuration for a specified interface. Specify the interface name.
on <DEVICE-NAME>	Optional. Displays MST configuration on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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

%   ge1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding
%   ge1: 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show startup-config {include-factory}
```

Parameters

```
show startup-config {include-factory}
```

startup-config include-factory	Displays startup configuration script • include-factory – Optional. Includes factory defaults

Examples

```
nx9500-6C8809#show startup-config
!
! Configuration of NX9500 version 7.1.0.0-010D
!
!
version 2.6
!
!
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"
!
mac access-list PERMIT-ARP-AND-IPv4
 permit any any type ip rule-precedence 10 rule-description "permit all IPv4 tra--More--
nx9500-6C8809#
```

t5

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 75XX, 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|wlam-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 • <T5-DEVICE-NAME> – Specify the T5 device's hostname. An error message is displayed if no T5 device name is specified.

```
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 *Customer Premises Equipment* (CPE) 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 • <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|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**, and **ge**.
	• dsl – Displays *Digital Subscriber Line* (DSL) interface related information
	• fe – Displays *Fast Ethernet* (FE) interface related information
	• ge – Displays *Gigabit Ethernet* (GE) 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. *Forward Error Correction* (FEC) 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	Selects A T5 controller's DSL interface. 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.
custom [avg|dses|dsses|peak|uses|usses]	Displays following custom CPE DSL data: • avg – Each DSL's average response time in microseconds • dses – The number of seconds downstream DSL transmissions were negatively impacted by code violations. • dsses – The number of seconds downstream DSL transmissions were severely negatively impacted by code violations. • peak – Each DSL's maximum (best to date since the screen was refreshed) response time in microseconds. • uses – The number of seconds upstream DSL transmissions were negatively impacted by code violations. • usses – The number of seconds upstream DLS transmissions were severely negatively impacted by code violations.
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 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>]	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. Use the following additional filters to filter on the basis of the VLAN or DSL interface: • dsl <1-24> – Filters information on the basis of the selected DSL port • ge <1-2> – Filters information on the basis of the selected GE port • vlan <1-4094 – Filters information on the basis of the selected VLAN port • wlan <1-24> – Filters on the basis of the selected CPE
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 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	Displays the T5 wireless client and WLAN related statistics • 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. Use the additional filters available to view specific client-related information. The options are: • association-status • authentication-status • bss • retry-percentage • rssi-value
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 wireless wlan counters [qos|rate|size] {on <T5-DEVICE-NAME>}
```

t5	Displays adopted T5 controller statistics
wireless wlan [qos|rate|size]	Displays the T5 wireless WLAN related statistics • wlan – Displays following T5 controller traffic counter statistics: • qos – Displays 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 • rates – Displays T5 controller's WLAN utilization data rate statistics Lists the number of data packets received and transmitted in the WLAN that have been relegated to a 1 Mbps data rate Lists the number of data packets received and transmitted in the WLAN by T5 controller connected devices at 54Mbps • size – Displays the number of data packets received and transmitted, in each listed WLAN, greater than 1024 bytes
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.

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    dsl1                   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     dsl2                    Wistron
Corp
```

```
--More--
nx9500-6C8809(config)#
```

terminal

Displays terminal configuration parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • class <1-4> – 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.
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 • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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#
```

tron (show command)

Displays the TRON-capable and TRON-enabled, WiNG AP's operating configuration.

Note

This command is applicable on TRON-capable, WiNG APs and controllers. And, the controller should have the TRON license applied, and TRON-capable and enabled AP(s) adopted to it.

Supported in the following platforms

- Access Points — AP-8533
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX 9000

Syntax

```
show tron operating-config {on <DEVICE-NAME>}
```

Parameters

```
show tron operating-config {on <DEVICE-NAME>}
```

show tron operating-config	Displays the operating configuration parameters
on <DEVICE-NAME>	Optional. Executes the command on a specified AP, controller, or service platform Following are the error outputs of this command: • `% Error: Not available under current working mode` **Note:** You will get this message, if the device (AP or controller) on which you have executed the command does not have TRON up and running, or does not support the TRON feature. • `TRON Operating Configuration: (none)` **Note:** You will get this message, when the FedEx backend server has not yet pushed the operating configuration to the WiNGAP. For more information on configuring TRON parameters, see tron on page 1161.

Examples

```
NOC-NX9500#show tron operating-config on ap8533-070154
TRON Operating Configuration:
  Device_Master_Type:                  0x00 (Fixed)
  Device_BLE_Scanner:                  xx:xx:xx:xx:xx:xx
  BLE_Scan_Type:                       0 (passive)
  BLE_Scan_Interval:                   16 (.625msec slots)
  BLE_Scan_Window:                     16 (.625msec slots)
  BLE_Own_Address_Type:                0 (public)
  BLE_Scan_Filter_Policy:              0 (accept_all)
  Node_Table_Monitor_Interval:         3 (seconds)
  Heartbeat_Interval:                  3 (minutes)
  Company_ID_List:                     0x0141
  Status_Change_Alert_Set_Enable:      0x00
  Status_Change_Alert_Clear_Enable:    0x00
  MQTT_Broker_Host:                    xx.xx.xx.xx
  MQTT_Broker_Port:                    1883
  MQTT_Topic_Publish_Prefix:           /TOPICS/PACKETS
  MQTT_Topic_Subscribe_Prefix:         /TOPICS/COMMANDS
  MQTT_QoS:                            2 (exactly_once)
  MQTT_Client_Id_Prefix:               FMN
  MQTT_Username:                       myname
  MQTT_Password:                       <encrypted string>
  MQTT_Clean_Session:                  0 (preserve_previous)
NOC-NX9500#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • on <DEVICE-NAME> – Optional. Displays last image upgrade status on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: If the 'on' keyword is used without the 'detail' keyword, the system displays a summary of upgrade status and log on the specified device.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 5.9.3.0-006D
Copyright (c) 2004-2018 Extreme Networks, Inc. All rights reserved.
Booted from primary

NOC-NX9500 uptime is 7 days, 00 hours 12 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#
```

```
ap8432-070235>show version
AP8432 version 5.9.3.0-007D
Copyright (c) 2004-2018 Extreme Networks, Inc. All rights reserved.
Booted from secondary

ap8432-070235 uptime is 0 days, 00 hours 04 minutes
CPU is ARMv7, No. of CPUs 2
Base ethernet MAC address is 74-67-F7-07-02-35
System serial number is 16009522200002
Model number is AP-8432-680B30-US

ap8432-070235>
```

vrrp

Displays *Virtual Router Redundancy Protocol* (VRRP)protocol details

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <1-255> – Optional. Displays information for a specified Virtual Router. Specify the router's ID from 1 -255.
on <DEVICE-NAME>	The following keyword is recursive and common to the '<1-255>' parameter: • on <DEVICE-NAME> – Optional. Displays specified router information on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 • on <DEVICE-NAME> – Optional. Displays global error statistics on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

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 *virtual-machine* (VM) configuration, logs, and statistics

Supported in the following platforms:

- Service Platforms — NX 95XX, NX 96XX

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: • VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. • team-urc – Optional. Displays TEAM-URC (IP-PBX) VM configuration/statistics • team-rls – Optional. Displays TEAM-RLS (Radio Link Server) VM configuration/statistics • team-vowlan – Optional. Displays TEAM-VoWLAN (Voice over WLAN) VM configuration/statistics
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

```
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| team-cmt]	The following keywords are common to the 'configuration' and 'statistics' parameters: • VM-NAME> – Optional. Displays VM configuration or statistics for the virtual machine identified by the <VM-NAME> keyword. Specify the VM name. • adsp – Optional. Displays *Air-Defense Services Platform* (ADSP) VM configuration/statistics • team-cmt – Optional. Displays TEAM-CMT VM configuration/statistics
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <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|info|warning]	Optional. Displays VM debugging logs based on the level selected. The available options are: • debug – Displays VM logs of level debug and above • error – Displays VM logs of level error • info – Displays VM logs of level Info and above • warning – Displays logs of level warning and above
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

```
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. The NX 95XX and NX 96XX series service platforms will display ADSP and TEAM-CMT VM configuration export information.
on <DEVICE-NAME>	Specifies the name of the device on which the command is executed • <DEVICE-NAME> – Specify the name of the service platform.

Examples

```
nx9500-6C874D#show virtual-machine statistics
--------------------------------------------------------------------------------
       NAME         STATE   VCPUS MEM (MB)    BRIDGE-IF             IP
--------------------------------------------------------------------------------
  WiNG             -         -     18432    -               -
  adsp             Halted    -     -        unknown         -
  team-cmt         Halted    -     -        unknown         -
--------------------------------------------------------------------------------
nx9500-6C874D#
nx9500-6C874D#show virtual-machine configuration
--------------------------------------------------------------------------------
           NAME               AUTOSTART         MEMORY(MB)          VCPUS
```

```
-------------------------------------------------------------------------------
  WiNG                      -                 18432              -
  adsp                      ignore            12000              12
  team-cmt                  ignore            1024               1
-------------------------------------------------------------------------------

nx9500-6C874D#
```

```
nx9500-6C874D>show virtual-machine statistics adsp
 VM name: adsp
 Base Version    : unknown
 Install Status  : not_installed
nx9500-6C874D>
```

wireless

Displays wireless configuration information and statistics

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
show wireless [ap|bridge|client|coverage-hole-incidents|location-server|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 location-server {on <AP-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|country-code|device-type]
show wireless regulatory [channel-info <CHANNEL-NUMBER>|country-code <COUNTRY-CODE>]
show wireless regulatory device-type [ap505|ap510i|ap510e|ap560i|ap560h]
[<COUNTRY-CODE>|avail-ant]
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 • <MAC/HOST-NAME> – Optional. Displays information for a specified AP. Specify the AP's MAC address.
on <DEVICE-OR-DOMAIN-NAME>}	The following keyword is recursive and common to the 'detail <MAC/HOST-NAME>' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
show wireless ap {load-balancing} {client-capability|events|neighbors} {(on <DEVICE-NAME>)}
```

wireless	Displays wireless configuration parameters
ap	Displays managed access point information
load-balancing {client-capability| events|neighbors}	Optional. Displays load balancing status. Use additional filters to view specific details. • client-capability – Optional. Displays client band capability • events – Optional. Displays client events • neighbors – Optional. Displays neighboring clients
on <DEVICE-NAME>	The following keyword is recursive and common to the 'client-capability', 'events', and 'neighbors' parameters: • on <DEVICE-NAME> – Optional. Displays load balancing information, based on the parameters passed, on a specified device • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform.

```
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 candidate-ap	Optional. Displays information about the candidate infrastructure access points as well as the infrastructure access point that the client-bridge radio has selected. Note: When enabled, the client-bridge radio scans its defined channels to locate the best candidate access point servicing the infrastructure WLAN.
<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. • <1-3> – Optional. Radio interface index if not specified as part of mesh ID.

filter radio-mac <RADIO-MAC>	This is a recursive parameter and common to all of the above options. • filter radio-mac – Optional. Provides additional filters to specifically identify the radio by its MAC address • <RADIO-MAC> – Specify the radio's MAC address.
on <DEVICE-OR-DOMAIN-NAME>	This is a recursive parameter and common to all of the above options. • on <DEVICE-OR-DOMAIN-NAME> – Optional. Executes the command on a specified device or devices within a specified RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the AP, controller, service platform, or RF Domain name.

```
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 • <DEVICE-NAME> – Specify the AP, controller, service platform name.

```
show wireless bridge {config}
```

wireless	Displays wireless configuration statistics
bridge config	Optional. Displays all client bridges in configuration 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 The output displays the configured client-bridges' host's MAC Address, bridge MAC address, IPv4 address, bridging status, and activity. Note: 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. • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name.

```
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 The output displays the signal, noise, SNR, TX/RX rates, retries, and errors.
traffic	Optional. Displays the client-bridge related traffic statistics 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 • on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the AP, controller, service platform, or Domain name.

```
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 • <MAC> – Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays association history on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail <MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <IP> – Selects clients with IP address matching the <IP> parameter • not <IP> – Inverts the match selection
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'IP' and 'not IP' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected wireless client information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • data-ready – Selects wireless clients in the data-ready state • not [data-ready|roaming] – Inverts match selection. Selects wireless clients neither ready nor roaming • Roaming – Selects roaming clients
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'ready', 'not', and 'roaming' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays selected client details on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <WLAN-NAME> – Specify the WLAN name. • not <WLAN-NAME> – Inverts the match selection
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'WLAN and 'not' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Filters clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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.
	• detail <MAC> – Optional. Displays detailed client statistics
	  • <MAC> – Optional. Displays detailed statistics for a specified client. Specify the client's MAC address.
	• rf – Optional. Displays detailed RF statistics on a specified device or RF Domain
	• window-data <MAC> – Optional. Displays historical data, for a specified client
	  • <MAC> – Optional. Specify the client's MAC address

on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail <MAC>', 'RF', and 'window-data <MAC>' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays client statistics, based on the parameters passed, on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <MAC> – Optional. Displays detailed TSPEC information for a specified client. Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN- NAME>	The following keyword is recursive and common to the 'tspec <MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed TSPEC information for wireless clients on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <MAC> – Optional. Displays detailed information for a specified wireless client. Specify the MAC address of the client.
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'detail <MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed information on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • filter – Optional. Defines additional filters. Use one of the following options to filter clients: ip, ipv6, state, and wlan. By default the system only displays the IPv4 address of clients. The include-ipv6 parameter includes the known IPv6 address of each client.
ip [<IPv4>|not <IPv4>]	Optional. Displays wireless client information based on the IPv4 address passed • <IPv4> – Displays information of the client identified by the <IPv4> parameter • not <IPv4> – Inverts the match selection
ipv6 [<IPv6>| not <Pv6>]	Optional. Displays wireless client information based on the IPv6 address passed • <IPv6> – Displays information of the client identified by the <IPv6> parameter • not <IPv6> – Inverts the match selection
filter state [data-ready|not [data-ready|roaming]|roaming]	Optional. Filters wireless client information based on their state • data-ready – Displays information of wireless clients in the data-ready state • not [data-ready|roaming] – Inverts match selection. Displays information of wireless clients neither ready nor roaming • Roaming – Displays information of roaming clients
wlan [<WLAN-NAME>| not <WLAN-NAME>]	Optional. Displays wireless client information based on the WLAN name passed • <WLAN-NAME> – Specify the WLAN name. • not <WLAN-NAME> – Inverts match selection

```
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/ HOSTNAME>| client-mac <MAC>]	Optional. Displays detailed coverage-hole related statistics • filters – Optional. Displays detailed coverage-hole related statistics on a per access point or wireless-client basis • ap <MAC/HOSTNAME> – Displays detailed coverage-hole related statistics for a specified access point <MAC/HOSTNAME> – Specify the access point's device name or MAC address. • client-mac <MAC> – Displays detailed coverage-hole related statistics encountered by a specified wireless client <MAC> – Specify the wireless client's MAC address Note: If the command is executed without any parameters being included, the system displays all coverage-hole related statistics.
summary	Optional. Displays a summary of coverage-hole related statistics
on <DOMAIN-NAME>	This parameter is recursive and is common to the 'detail' and 'summary' keywords: • on <DOMAIN-NAME> – Optional. Displays detailed or summary coverage-hole related statistics on a specified RF Domain • <DOMAIN-NAME> – Specify the domain name.

```
show wireless location-server {on <AP-NAME>}
```

show wireless location-server on <AP-NAME>	Displays location server connection status on a specified access point • <DEVICE-NAME> - Specify the AP name.

```
show wireless meshpoint {config} {filter [device <DEVICE-NAME>|rf-domain <DOMAIN-NAME>]}
```

wireless	Displays wireless configuration parameters.
meshpoint	Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area. 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.
config	Optional. Displays all meshpoint configuration
filters [device <DEVICE-NAME>| rf-domain <DOMAIN-NAME>]	Optional. Provides additional filter options, such as device name and RF Domain name. • device <DEVICE-NAME> – Displays meshpoints applied to a specified device • <DEVICE-NAME> – Specify the device name • rf-domain <DOMAIN-NAME> – Displays meshpoints applied to a specified RF Domain • <DOMAIN-NAME> – Specify the domain name

```
show wireless meshpoint {detail} {<MESHPOINT-NAME>}
```

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area. 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 <MESHPOINT-NAME>	Optional. Displays detailed information for all meshpoints or a specified meshpoint • <MESHPOINT-NAME> – Optional. Displays detailed information for a specified meshpoint. Specify the meshpoint name.

```
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. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area. 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: • <MESHPOINT-NAME> – Displays meshpoint related information for a specified meshpoint. Specify the meshpoint name. • detail – Displays detailed multicast information for all meshpoints
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed multicast information on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
show wireless meshpoint {neighbor} [<MESHPOINT-NAME>|detail|statistics {rf}]
{on <DEVICE-OR-DOMAIN-NAME>}
```

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information. Use this option to view detailed statistics on each Mesh-capable client available within controller's adopted access point's radio coverage area. 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.
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 • <MESHPOINT-NAME> – Displays detailed multicast information for a specified meshpoint. Specify the meshpoint name. • detail – Displays detailed multicast information for all meshpoints • statistics – Displays neighbors related statistics • rf – Optional. Displays RF related statistics for neighbors
on <DEVICE-OR-DOMAIN- NAME>	The following keyword is common to all of the above parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays meshpoint neighbor information, based on the parameters passed, on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
show wireless meshpoint {tree} {on <DEVICE-OR-DOMAIN- NAME>}
```

wireless	Displays wireless configuration parameters
meshpoint	Displays meshpoint related information **Note:** The `show > wireless > meshpoint > tree` 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 • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain

```
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 • <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of AP, wireless controller, service platform, or RF Domain

```
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: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • 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. • detail – Displays detailed MiNT-mesh related information
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 • <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name.

```
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 • <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name.

```
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 • <DEVICE-OR-DOMAIN-NAME> – Specify the access point, controller, or RF Domain name.

```
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 *Signal to Noise Ratio* (SNR). This data is reported to the managing controller or service platform from connected access point radios and should be refreshed periodically. A radio's RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation
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 • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN-NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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. A radio's RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation
detail	Optional. Displays detailed radio operation status
filter <RADIO-MAC>	Optional. Provides additional filter options • <RADIO-MAC> – Uses MAC address to filter radios
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is recursive and common to the 'filter <RADIO-MAC>' parameter: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays detailed radio operation status for all or a specified radio on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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. A radio's RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation
statistics	Optional. Displays radio traffic and RF statistics

on <DEVICE-OR-DOMIAN- NAME>	Optional. Displays traffic and RF related statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
rf {on <DEVICE-OR-DOMAIN-NAME>}	Optional. Displays RF statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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. A radio's RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation
statistics {detail|window-data}	Optional. Displays radio traffic and RF statistics. Use additional filters to view specific details. The options are: are: • detail – Displays detailed traffic and RF statistics of all radios • window-data – Displays historical data over a time window
<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 • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN- NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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. A radio's RF Mode displays as: • 2.4GHz-wlan – If it is configured to provide 2.4 GHz WLAN service • 5GHz-wlan – If it is configured to provide 5.0 GHz WLAN service • bridge – If it is configured to provide client-bridge operation
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 • <RADIO-MAC> – Optional. Filters based on the radio MAC address
on <DEVICE-OR-DOMAIN- NAME>	Optional. After specifying the radio MAC address, further refine the search by specifying a device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
show wireless regulatory [channel-info <CHANNEL-NUMBER>|country-code <COUNTRY-CODE>]
```

wireless regulatory	Displays wireless regulatory information
channel-info <WORD>	Displays channel information based on the channel number specified. • <WORD> – Specify the channel number.
country-code <WORD>	Lists the supported country codes • <WORD> – Specify the two letter ISO-3166 country code.

```
show wireless regulatory device-type [ap505|ap510i|ap510e|ap560i|ap560h]
[<COUNTRY-CODE>|avail-ant]
```

wireless regulatory	Displays wireless regulatory information
device-type <DEVICE-TYPE>	Displays supported antenna types based on the device type selected. • <DEVICE-TYPE> - Specify the device type. The options are: ap505, ap510i, ap510e, ap560i, and ap560h.
<COUNTRY-CODE> <ANTENNA-TYPE>	Displays channel-wise power and DFS settings based on the country code and antenna-type selected. • <ANTENNA-TYPE> - Configures the antenna type. Displays the supported power based on the country code and antenna type specified. Note: The <ANTENNA-TYPE> parameter is applicable only for the AP510i/e and AP560i/h model access points.
avail-ant	Displays the antenna types available for the selected device type.

```
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: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays RF Domain statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays AirDefense sensor server configuration on a specified device or RF Domain

```
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: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Specify the name of the 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.

```
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 • client-blacklist – Displays blacklisted clients • event-history – Displays event history
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'client-blacklist' and 'event-history' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays the WIPS details on a specified device or RF Domain. • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

```
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 • <WLAN> – Specify the WLAN name.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays WLAN configuration on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
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 • <DEVICE-NAME> – Specify the device name.
rf-domain <DOMAIN-NAME>	Optional. Filters WLAN information based on the RF Domain • <DOMAIN-NAME> – Specify the RF Domain name.

```
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 • <WLAN> – Specify the WLAN name.
on <DEVICE-OR-DOMAIN-NAME>	Optional. Displays WLAN configuration on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.
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 • <DEVICE-NAME> – Specify the device name.
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 • <WLAN> – Optional. Displays WLAN statistics. Specify the WLAN name. • detail – Optional. Displays detailed WLAN statistics
on <DEVICE-OR-DOMAIN-NAME>	The following keyword is common to the 'WLAN' and 'detail' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays WLAN statistics on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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#show wireless regulatory country-code
------------------------------------------------------------------------------
            ISO CODE                                    NAME
------------------------------------------------------------------------------
  gt                            Guatemala
  co                            Colombia
  cn                            China
  cm                            Cameroon
  cl                            Chile
  al                            Albania
  ca                            Canada
  gy                            Guyana
  hu                            Hungary
--More--
nx9500-6C8809#
nx9500-6C8809#show wireless regulatory device-type ap505 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       1000      30          Indoor/Outdoor   Required       1       Required
  4   52-64       500       27          Indoor/Outdoor   Required       1       Not
Required
  5   100-140     1000      30          Indoor/Outdoor   Required       1       Required
  6   100-140     500       27          Indoor/Outdoor   Required       1       Not
Required
  7   149-165     4000      36          Indoor/Outdoor   Not Required   0       Not
Required
```

```
-------------------------------------------------------------------------------------------------
---
nx9500-6C8809#
ap505-13403B(#show wireless client
-------------------------------------------------------------------------------------------------
------
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
-------------------------------------------------------------------------------------------------
-------
Total number of clients displayed: 2
ap505-13403B(#
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)#
```

The following example shows the location-server status as online:

```
vx9000-739FF8#show wireless location-server on ap7532-1600B0
-------------------------------------------------------------------------------
  #              LOCATION SERVER HOST            PORT         STATUS
-------------------------------------------------------------------------------
  1          testws.extremelocation.com          443          ONLINE
-------------------------------------------------------------------------------
vx9000-739FF8#
```

If the location-server IP address/hostname is not configured in the AP's RF-Domain, then the status displays as "no server defined" as shown in the following example:

```
vx9000-739FF8(config)#show wireless location-server on ap505-13403B
-------------------------------------------------------------------------------
  #          LOCATION SERVER HOST        PORT               STATUS
-------------------------------------------------------------------------------
  1                                      0           no server defined
-------------------------------------------------------------------------------
vx9000-739FF8(config)#
ap505-133E1C#show wireless regulatory country-code
-------------------------------------------------------------------------------
               ISO CODE                                NAME
-------------------------------------------------------------------------------
  BE                                BELGIUM
  FR                                FRANCE
  BG                                BULGARIA
  GR                                GREECE
  EE                                ESTONIA
  CA                                CANADA
  DE                                GERMANY
  IT                                ITALY
  HU                                HUNGARY
```

```
  CZ                                CZECH REPUBLIC
  CY                                CYPRUS
  CH                                SWITZERLAND
  AU                                AUSTRALIA
  AT                                AUSTRIA
  FI                                FINLAND
  NZ                                NEW ZEALAND
  IE                                IRELAND
  ES                                SPAIN
  DK                                DENMARK
  LV                                LATVIA
--More--
ap505-134038#
--------------------------------------------------------------------------------
ap505-133E1C#
ap505-134038#show wireless re device-type ap505 us
--------------------------------------------------------------------------------------------------
  #   Channel Set Power(mW) Power (dBm) Placement      DFS       CAC(mins)      TPC
--------------------------------------------------------------------------------------------------
  1    1-1         160       22          Indoor    Not Required   0         Not Required
  2    2-8         200       23          Indoor    Not Required   0         Not Required
  3    9-9         160       22          Indoor    Not Required   0         Not Required
  4    10-11       125       21          Indoor    Not Required   0         Not Required
  5    36-36       100       20          Indoor    Not Required   0         Not Required
  6    40-48       250       24          Indoor    Not Required   0         Not Required
  7    149-149     200       23          Indoor    Not Required   0         Not Required
  8    153-153     250       24          Indoor    Not Required   0         Not Required
  9    157-161     320       25          Indoor    Not Required   0         Not Required
--More--
ap505-134038#
ap505-134038#show wireless regulatory device-type ap505 antenna
--------------------------------------------------------------------------------
           RADIO                      Band                    Antenna
--------------------------------------------------------------------------------
  radio-1                    2.4G                    internal
  radio-2                    5.0G                    internal
--------------------------------------------------------------------------------
ap505-134038#
ap505-134038#show wireless regulatory device-type ap510i antenna
--------------------------------------------------------------------------------
           RADIO                      Band                    Antenna
--------------------------------------------------------------------------------
  radio-1                    2.4G                    internal
  radio-1                    5.0G                    internal
  radio-2                    5.0G                    internal
--------------------------------------------------------------------------------
ap505-134038#
ap510-133AAA(config-device-94-9B-2C-13-3A-AA)#show wireless radio
--------------------------------------------------------------------------------------------------
---------------
RADIO               RADIO-MAC             RF-MODE        STATE
CHANNEL    POWER #CLIENT
--------------------------------------------------------------------------------------------------
---------------
ap510-133AAA:R1      94-9B-2C-0E-66-20 2.4GHz-wlan          Off              N/A (  smt)
0 (smt)       0
ap510-133AAA:R2      94-9B-2C-0E-66-30   5GHz-wlan           On               36 (   36)
15 (smt)       0
--------------------------------------------------------------------------------------------------
---------------
```

```
Total number of radios displayed: 2
ap510-133AAA(config-device-94-9B-2C-13-3A-AA)#
ap510-133C9B#show wireless regulatory channel-info
-------------------------------------------------------------------------------
             CHANNEL                          Center Frequency(MHz)
-------------------------------------------------------------------------------
  1                                2412
  2                                2417
  3                                2422
  4                                2427
  5                                2432
  6                                2437
  7                                2442
  8                                2447
  9                                2452
  10                               2457
  11                               2462
  12                               2467
  13                               2472
  14                               2484
  21                               4955
  25                               4975
  34                               5170
  36                               5180
  38                               5190
  40                               5200
  42                               5210
--More--
ap510-133C9B#

ap510-133C9B#show wireless regulatory country-code
-------------------------------------------------------------------------------
             ISO CODE                                    NAME
-------------------------------------------------------------------------------
  BE                               BELGIUM
  FR                               FRANCE
  BG                               BULGARIA
  BA                               BOSNIA & HERZEGOVIN
  BM                               BERMUDA
  JP                               JAPAN
  BF                               BURKINA_FASO
  BJ                               BENIN
  BW                               BOTSWANA
  BR                               BRAZIL
  BS                               BAHAMAS
  FI                               FINLAND
  FK                               FALKLAND_ISLANDS
  FM                               MICRONESIA
  AL                               ALBANIA
  RU                               RUSSIA
  NL                               NETHERLANDS
  NO                               NORWAY
  KY                               CAYMAN_ISLANDS
  RE                               REUNION
  NZ                               NEW ZEALAND
--More--
ap510-133C9B#
ap510-133C9B#show wireless regulatory device-type ap510e us
-------------------------------------------------------------------------------
  #   Channel Set Power(mW) Power (dBm) Placement      DFS          CAC(mins)
-------------------------------------------------------------------------------
  1    1-1         80        19          Indoor    Not Required   0
  2    2-3         100       20          Indoor    Not Required   0
  3    4-7         125       21          Indoor    Not Required   0
```

```
  4    8-9         100       20          Indoor    Not Required   0
  5    10-10       80        19          Indoor    Not Required   0
  6    11-11       64        18          Indoor    Not Required   0
  7    1-1         80        19          Outdoor   Not Required   0
  8    2-3         100       20          Outdoor   Not Required   0
  9    4-7         125       21          Outdoor   Not Required   0
  10   8-9         100       20          Outdoor   Not Required   0
  11   10-10       80        19          Outdoor   Not Required   0
  12   11-11       64        18          Outdoor   Not Required   0
  13   36-36       32        15          Indoor    Not Required   0
  14   40-44       64        18          Indoor    Not Required   0
  15   48-48       50        17          Indoor    Not Required   0
  16   36-48       20        13          Outdoor   Not Required   0
  17   149-149     80        19          Indoor    Not Required   0
  18   153-169     125       21          Indoor    Not Required   0
  19   149-149     80        19          Outdoor   Not Required   0
  20   153-169     125       21          Outdoor   Not Required   0
--More--
ap510-133C9B#
ap510-133C9B#show wireless regulatory device-type ap510e antenna
------------------------------------------------------------------------------
         RADIO                  Band                      Antenna
------------------------------------------------------------------------------
  radio-1               2.4G              ml-2452-hpag4a6-01
  radio-1               2.4G              ml-2452-hpa5-036
  radio-1               2.4G              ml-2452-apa2-01
  radio-1               2.4G              ml-2452-apa2-02
  radio-1               2.4G              ml-2452-pna5-01r
  radio-1               2.4G              ml-2452-hpag5a8-01
  radio-1               2.4G              ml-2452-pta4m4-036
  radio-1               2.4G              ws-ai-dq05120
  radio-1               2.4G              ai-dq04360s
  radio-1               2.4G              ml-2452-pna7-01r
  radio-1               2.4G              ml-2452-sec6m4-036
  radio-1               5.0G              ml-2452-pna5-01r
  radio-1               5.0G              ml-2452-apa2-01
  radio-1               5.0G              ml-2452-apa2-02
  radio-1               5.0G              ml-2452-hpag5a8-01
  radio-1               5.0G              ml-2452-pta4m4-036
  radio-1               5.0G              ml-2452-sec6m4-036
  radio-1               5.0G              ws-ai-dq05120
  radio-1               5.0G              ml-2452-hpag4a6-01
  radio-1               5.0G              ml-2452-hpa5-036
  radio-1               5.0G              ai-dq04360s
  radio-1               5.0G              ml-2452-pna7-01r
  radio-2               5.0G              ml-2452-pna5-01r
  radio-2               5.0G              ml-2452-apa2-01
  radio-2               5.0G              ml-2452-apa2-02
  radio-2               5.0G              ml-2452-hpag5a8-01
  radio-2               5.0G              ml-2452-pta4m4-036
  radio-2               5.0G              ml-2452-sec6m4-036
  radio-2               5.0G              ws-ai-dq05120
  radio-2               5.0G              ml-2452-hpag4a6-01
  radio-2               5.0G              ml-2452-hpa5-036
  radio-2               5.0G              ai-dq04360s
  radio-2               5.0G              ml-2452-pna7-01r
------------------------------------------------------------------------------
ap510-133C9B#
ap510-133C9B#show wireless radio wlan-map on ap510-133C9B
------------------------------------------------------------------------------------------
----
RADIO                AP-MAC            AP-TYPE      RF-MODE BSS WLAN MAPPED
                                                           IDX
------------------------------------------------------------------------------------------
```

```
----
ap510-133C9B:R1      94-9B-2C-13-3C-9B ap510    2.4GHz-wlan 1   wlan1*
ap510-133C9B:R2      94-9B-2C-13-3C-9B ap510      5GHz-wlan 1   wlan1*
-------------------------------------------------------------------------------------------
----
ap510-133C9B#
ap510-133C9B#show wireless radio detail ap510-133C9B

Radio: 94-9B-2C-13-3C-9B:R1, alias ap510-133C9B:R1
 STATE                : Off [regulatory power requirement]
 PHY INFO             : Bssid: 94-9B-2C-0E-72-A0 RF-Mode: 2.4GHz-wlan
 ACCESS POINT         : Name: ap510-133C9B  Location: default  Placement: Indoor
 CHANNEL              : Current: N/A Configured: smt Width: 20MHz
 TRANSMIT POWER       : 0 dBm
 ANTENNA USAGE        : 4x4
 MAXIMUM DATA RATES   : Phy: N/A User: N/A
 PHY SETTINGS         : Short Preamble: N Dual Channel: N Spectrum Mgmt: N
 RATE SELECTION       : Standard
 ANTENNA DOWNTILT     : Not-Supported
 RADIO SHARE MODE     : Off
 TRANSMIT BEAMFORMING : Enabled
 MU-MIMO              : Disabled
 SCAN_AHEAD CHANNEL   : -
 ERP COEXISTENCE      : ERP Protection: N Non-ERP detected: N Non-ERP associated: N
 HT COEXISTENCE       : HT Protection: no-protection, Non-HT detected: N
 Current Channel Width: 20Mhz, reason: per configuration
 Num of Mcast Streams : 0 (max:25)
 Multicast streams    :
 WLAN MAP             :
     BSS-1            : wlan1* (*=primary)(BSSID : 94-9B-2C-0E-72-A0)
     Shutdown WLANs   :
 BSS MAP              :
     BSS-1            : basic-rates    = 1 2 5.5 11
                      : supported-rates= 1 2 5.5 6 9 11 12 18 24 36 48 54 mcs-1s mcs-2s
mcs-3s mcs-4s
 Last error           :
--More--
ap510-133C9B#
ap510-133C9B#show wireless regulatory device-type ap510e fr ml-2452-hpa5-036
-------------------------------------------------------------------------------
  #   Channel Set Power(mW) Power (dBm) Placement      DFS          CAC(mins)
-------------------------------------------------------------------------------
  1    1-13        25        14          Indoor    Not Required   0
  2    1-13        25        14          Outdoor   Not Required   0
  3    36-48       32        15          Indoor    Not Required   0
  4    52-64       32        15          Indoor    Required       1
  5    100-100     50        17          Indoor    Required       1
  6    104-116     64        18          Indoor    Required       1
  7    100-100     50        17          Outdoor   Required       1
  8    104-116     64        18          Outdoor   Required       1
  9    120-128     64        18          Indoor    Required       10
  10   120-128     64        18          Outdoor   Required       10
  11   132-140     64        18          Indoor    Required       1
  12   132-140     64        18          Outdoor   Required       1
-------------------------------------------------------------------------------
ap510-133C9B#
ap560-135500#show wireless regulatory device-type ap560h us internal-560h-30
-------------------------------------------------------------------------------
  #   Channel Set Power(mW) Power (dBm) Placement      DFS          CAC(mins)
-------------------------------------------------------------------------------
  1    1-1         125       21          Indoor    Not Required   0
  2    2-10        200       23          Indoor    Not Required   0
  3    11-11       125       21          Indoor    Not Required   0
```

```
  4    1-1         125       21          Outdoor   Not Required   0
  5    2-10        200       23          Outdoor   Not Required   0
  6    11-11       125       21          Outdoor   Not Required   0
  7    36-36       80        19          Indoor    Not Required   0
  8    40-44       125       21          Indoor    Not Required   0
  9    48-48       80        19          Indoor    Not Required   0
  10   36-48       40        16          Outdoor   Not Required   0
  11   149-153     250       24          Indoor    Not Required   0
  12   157-161     320       25          Indoor    Not Required   0
  13   165-165     200       23          Indoor    Not Required   0
  14   149-153     250       24          Outdoor   Not Required   0
  15   157-161     320       25          Outdoor   Not Required   0
  16   165-165     200       23          Outdoor   Not Required   0
-------------------------------------------------------------------------------
```

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 75XX, 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: • basic – Displays all category types configured for the basic filter-level • high – Displays all category types configured for the high filter-level • low – Displays all category types configured for the low filter-level • medium – Displays all category types configured for the medium filter-level • medium-high – Displays all category types configured for the medium-high filter-level
statistics {on <DEVICE-NAME>}	Displays Web filter statistics on a specified device • on <DEVICE-NAME> – Optional. Specifies the device name • <DEVICE-NAME> – Specify the name of the AP, controller, or service platform. Note: Web filtering is a licensed feature, and only when enforced can the system display Web filtering statistics.
status {on <DEVICE-NAME>}	Displays Web filter status on a specified device • on <DEVICE-NAME> – Optional. Specifies the device name • <DEVICE-NAME> – Specify the name of the AP, controller, or service platform. Note: Web filtering is a licensed feature, and only when enforced can the system display Web filtering status.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <WORD> – Specify the string to use as match criteria (for example, MAC address, hostname, etc.).
is <WORD>	Searches for items exactly matching a specified string • Specify the string to use as match criteria (for example, MAC address, hostname, etc.).
on <DEVICE-OR-DOMAIN-NAME>	Optional. Performs global search on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the name of the AP, wireless controller, service platform, or RF Domain.

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                      NAME/VALUE
------------------------------------------------------------------------------------------------
------------------------------------------------------------

                          https-trustpoint                 type
mac                             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
```

```
                          qos_policy                      name
control_vlan                    beacon_format

--More--
rfs4000-229D58#
```

wwan

Displays wireless WAN status

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	The following keyword is common to the 'configuration' and 'status' parameters: • on <DEVICE-OR-DOMAIN-NAME> – Optional. Displays configuration or status details on a specified device or RF Domain • <DEVICE-OR-DOMAIN-NAME> – Specify the AP, wireless controller, service platform, or RF Domain name.

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)#
```

8 Profiles

Profile Config Commands
Device Config Commands

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 1326.

A user-defined profile can be created for each of the following device type:

- AP505 - Adds an AP505 access point profile
- AP510 - Adds an AP510 access point profile
- AP560 - Adds an AP560 access point profile
- NX5500 – Adds an NX5500 wireless controller profile
- NX75XX – Adds an NX7500 series service platform profile
- NX9000 – Adds an NX9500 series service platform profile
- NX9600 – Adds an NX9600 series service platform profile
- VX9000 – Adds a VX9000 virtual controller profile

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 853
- Device Config Commands on page 1265

To view the list of device profiles supported, use the following command:

```
<DEVICE>(config)#profile ?

nx9500-6C8809#configure
Enter configuration commands, one per line.  End with CNTL/Z.
nx9500-6C8809(config)#profile ?
  anyap       Any access point profile
  ap505       AP505 access point profile
  ap510       AP510 access point profile
  ap560       AP560 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 ap505 default-ap505
nx9500-6C8809(config-profile-default-ap505)#

<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>
<DEVICE>(config-profile-<PROFILE-NAME>)#

nx9500-6C8809(config)#profile ap510 default-ap510
ap510-133C9B(config-profile-default-ap510)#?
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
  antenna-id                               Configure the antenna on the AP
  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
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  controller                               WLAN controller configuration
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  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
  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
  led                                      Turn LEDs on/off on the device
  legacy-auto-downgrade                    Enable device firmware to auto
                                           downgrade when other legacy devices
```

```
                                        are detected
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
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
ntp                                     Ntp server WORD
offline-duration                        Set duration for which a device
                                        remains unadopted before it
                                        generates offline event
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
purview-application-policy              Purview application policy
                                        configuration
radius                                  Configure device-level radius
                                        authentication parameters
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
spanning-tree                           Spanning tree
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
virtual-controller                      Enable Controller AP
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
ws-controller                           Configure websocket controller
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

ap510-133C9B(config-profile-default-ap510)#


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 34: Profiles Config Mode Commands

Command	Description
adopter-auto-provisioning-policy-lookup on page 857	Enables the use of a centralized auto provisioning policy on this profile
adoption on page 857	Configures a minimum and maximum delay time in the initiation of the device adoption process
adoption-mode on page 858	Sets the adoption mode for access points to Controller, cloud, or Extreme Services
alias on page 865	Creates various types of aliases, such as network, VLAN, network-group, network-service, encrypted-string, hashed -string, etc. at the profile level
antenna-id (ap510e) on page 861	Configures the antenna ID in the AP510e model access point profile and device contexts. Use this command to specify the antenna group and enable the access point radios.
antenna-id (ap560h) on page 864	Configures the antenna ID in the AP560h model access point profile and device contexts. Use this command to specify which internal antenna to use (30/70 degree) and enable the access point radios.
application-policy on page 875	Enables the RADIUS *Change of Authorization* (CoA) mechanism. Reinitiates authentication and changes attributes of active AAA session based on the rules defined by the application policy specified here. Note: Supported only on WiNG 5.9.X devices.
area on page 876	Sets the system's area of location (the area name)
arp on page 877	Configures static address resolution protocol
auto-learn on page 879	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.
autogen-uniqueid on page 880	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.
autoinstall on page 881	Configures the automatic install feature
bridge on page 883	Configures bridge specific parameters
captive-portal on page 910	Configures captive portal advanced Web page upload on a device profile
cdp on page 911	Enables *Cisco Discovery Protocol* (CDP) on a device

Table 34: Profiles Config Mode Commands (continued)

Command	Description
cluster on page 912	Configures a cluster name
configuration-persistence on page 914	Enables persistence of configuration across reloads
controller on page 915	Configures a wireless controller or service platform
critical-resource on page 920	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.
crypto on page 929	Configures data encryption related protocols and settings
database on page 976	Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value
device-onboard on page 977	Configures the logo image file name and title displayed on the ExtremeGuest device-onboarding portal. This is the portal a vendor-admin user uses to onboard devices.
device-upgrade on page 978	Configures device firmware upgrade settings on this profile
diag on page 980	Enables looped packet logging
dot1x on page 981	Configures 802.1x standard authentication controls
dpi on page 983	Enables *Deep Packet Inspection* (DPI) on this profile
dscp-mapping on page 986	Configures an IP DSCP to 802.1p priority mapping for untagged frames
eguest-server (VX9000 only) on page 987	Enables the EGuest daemon when executed without the 'host' option
eguest-server (NOC Only) on page 988	Points to the EGuest server, when executed along with the 'host' option
email-notification on page 989	Configures e-mail notification settings
enforce-version on page 991	Enables checking of a device's firmware version before attempting adoption or clustering
environmental-sensor on page 992	Configures the environmental sensor settings on this profile (applicable to AP8132 model access point only)
events on page 994	Enables system event logging and message generation. This command also configures event message forwarding settings.
export on page 994	Enables export of startup.log file after every boot
file-sync on page 995	Configures parameters enabling synching of trustpoint and/or wireless-bridge certificate between the staging-controller and adopted access point
floor on page 997	Sets the floor name where the system is located
gre on page 997	Enables *Generic Routing Encapsulation* (GRE) tunneling on this profile
http-analyze on page 1007	Configures HTTP analysis settings
interface on page 1009	Configures an interface (VLAN, radio, GE, etc.)
ip on page 1167	Configures IPv4 components
ipv6 on page 1175	Configures IPv6 components

Table 34: Profiles Config Mode Commands (continued)

Command	Description
l2tpv3 on page 1180	Defines the *Layer 2 Tunnel Protocol* (L2TP) for tunneling layer 2 payloads using *Virtual Private Networks* (VPNs)
l3e-lite-table on page 1182	Configures L3e Lite Table with this profile
led on page 1183	Turns device LEDs on or off
led-timeout on page 1184	Configures LED-timeout timer. This command is specific to the NX9500 series service platforms.
legacy-auto-downgrade on page 1185	Auto downgrades a legacy device firmware
legacy-auto-update on page 1185	Auto upgrades a legacy device firmware
lldp on page 1186	Configures *Link Layer Discovery Protocol* (LLDP) settings
load-balancing on page 1187	Configures load balancing parameters
logging on page 1193	Modifies message logging settings
mac-address-table on page 1195	Configures the MAC address table
mac-auth on page 1197	Enables 802.1x user authentication protocol on this profile
management-server on page 1199	Configures a management server with this profile
meshpoint-device on page 1200	Configures meshpoint device parameters
meshpoint-monitor-interval on page 1201	Configures meshpoint monitoring interval
min-misconfiguration-recovery-time on page 1202	Configures the minimum device connectivity verification time
mint on page 1203	Configures MiNT protocol settings
misconfiguration-recovery-time on page 1211	Verifies device connectivity after a configuration is received
neighbor-inactivity-timeout on page 1212	Configures neighbor inactivity timeout
neighbor-info-interval on page 1213	Configures neighbor information exchange interval
no on page 1214	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.
noc on page 1216	Configures NOC settings
nsight on page 1217	Configures NSight database related parameters
ntp on page 1221	Configures NTP server settings
otls on page 1224	Configures support for detection and forwarding of OmniTrail beacon tags
offline-duration on page 1226	Sets the duration, in minutes, for which a device remains un-adopted before it generates offline event
power-config on page 1227	Configures the power mode
preferred-controller-group on page 1229	Specifies the wireless controller or service platform group preferred for adoption

Table 34: Profiles Config Mode Commands (continued)

Command	Description
preferred-tunnel-controller on page 1230	Configures the tunnel wireless controller or service platform preferred by the system to tunnel extended VLAN traffic
purview-application-policy on page 1230	Enables the RADIUS *Change of Authorization* (CoA) mechanism. Reinitiates authentication and changes attributes of active AAA session based on the rules defined by the purview application policy specified here. Note: Supported only on WiNG 7.1.2 APs.
radius on page 1231	Configures device-level RADIUS authentication parameters
raid on page 1301	Enables alarm on the array. This command is supported only on the NX9500 series service platform profile/device config modes.
rf-domain-manager on page 1232	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.
router on page 1233	Configures dynamic router protocol settings
spanning-tree on page 1235	Configures spanning tree related settings
traffic-class-mapping on page 1238	Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority
traffic-shape on page 1239	Enables traffic shaping and configures traffic shaping parameters
trustpoint (profile-config-mode) on page 1245	Configures the trustpoint assigned for validating a CMP auth Operator
tunnel-controller on page 1246	Configures the name of tunneled WLAN (extended VLAN) wireless controller or service platform
use (profile/device-config-mode-commands) on page 1247	Uses pre configured policies with this profile
vrrp on page 1253	Configures *Virtual Router Redundancy Protocol* (VRRP) group settings
vrrp-state-check on page 1257	Publishes interface via OSPF or BGP based on VRRP status
wep-shared-key-auth on page 1257	Enables support for 802.11 WEP shared key authentication
ws-controller on page 1258	Configures multiple ws-controller hosts and enables rediscovery of new controllers. This option is required for WiNG APs with 'adoption-mode' set to 'ws-controller'. That is WiNG APs adopting to the ExtremeCloud Appliance controller.
service on page 1259	Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.
zone on page 1265	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 616.

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 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • evaluate-always – Optional. Sets flag to run centralized auto-provisioning policy every time a device (access point/controller) is adopted.

Examples

```
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 1214	Disables the application of centralized auto provisioning policy on this profile or device

adoption

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
adoption start-delay min <0-30> max <0-30>
```

Parameters

```
adoption start-delay min <0-30> max <0-30>
```

adoption start-delay min <0-30> max <0-30>	Delays start of the device adoption process • min <0-30> – Configures the minimum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds. A device, on coming up, attempts adoption only after the lapse of the time specified here. The default is 5 seconds. • max <0-30> – Configures the maximum time to lapse before a device attempts adoption. Specify a value from 0 - 30 seconds. The default is 20 seconds.

Example

```
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

no on page 1214	Removes the configured minimum start-delay value. When removed, devices attempt adoption immediately on coming up.

adoption-mode

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
adoption-mode [cloud|controller|ws-controller]
```

Parameters

```
adoption-mode [cloud|controller|ws-controller]
```

adoption-mode [cloud|controller|ws-controller]	Use to set the adoption-mode to:
	• 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.
	• controller – Sets the adoption mode to the local WiNG controller. This is the default setting. Note, APs with the 'controller > host > configuration' specified are marked as local-controller APs and never try adopting to the CLOUD or WS-Controller
	• 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 management-server on page 1199.
	
	Note: 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:
	In the DHCP server policy, define an alias for option 191:
	`VX(config-dhcp-policy-DHCP)#`
	` dhcp-server-policy DHCP`
	`  option AP-adoption 191 ascii`
	In the DHCP pool config, define the option 191 string:
	`dhcp-pool AP`
	`  option AP-adoption pool1=<ws-controller-ip-adress>;`
	`adoption-mode=ws-controller`

Examples

```
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 radio1
 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)#
ap505-13403B(config-device-94-9B-2C-13-40-38)#aadoption-mode ws-controller
ap505-13403B(config-device-94-9B-2C-13-40-38)#show context
ap505 94-9B-2C-13-40-38
 use profile default-ap505
 use rf-domain default
 hostname ap505-13403B
 mint mlcp vlan
 mint mlcp ip
 ip default-gateway 10.234.160.254
 ip route 134.141.244.0/24 10.234.160.254
 ip route 10.233.84.0/24 10.234.160.254
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 10.234.160.36/24
 logging on
 logging console debugging
 adoption-mode ws-controller
ap505-13403B(config-device-94-9B-2C-13-40-38)#
```

Related Commands

no on page 1214	Reverts the adoption-mode to default (controller)

antenna-id (ap510e)

Profile Config Commands on page 853

Configures the antenna ID on an AP510e model access point profile and device. Use this command to specify the antenna types used with the external antennas.

The ExtremeMobility AP510e access point is a dual-radio access point, with eight, external Wi-Fi antennas grouped into: group-1 (antenna ports 1 to 4) and group-2 (antenna ports 5 to 8).

To enable the AP510e radio, configure the country code, map a WLAN to the radio, and configure the *antenna-id* for the 'group-1' and 'group-2' antenna ports. The antenna-id parameter, specifies the antenna type used in the group-1 and/or group-2 antenna ports.

	Antenna Ports	
Software Mode	**2.4/5G Antennas: 1, 2, 3, 4**	**5G Antennas: 5, 6, 7, 8**

Mode 1 • Radio 1 - 2.4 GHz WLAN • Radio 2 - 5 GHz WLAN Note: This mode requires only *FOUR, dual-band* antennas connected to ANT sockets 1 to 4. Note: If using this mode, configure antenna-id only for the group 1 antennas.	Dual-band 2.4 GHz/5 GHz	None
Mode 2 • Radio 1 - 2.4/5 GHz Sensor • Radio 2 - 5 GHz WLAN Note: This mode requires *FOUR, dual-band* antennas connected to ANT sockets 1 to 4, and *FOUR, 5G-band* antennas connected to ANT sockets 5 to 8. Note: If using this mode, configure antenna-id for both group 1 and group 2 antennas.	Dual-band 2.4 GHz/5 GHz	5 GHz
Mode 3 • Radio 1 - 5 GHz WLAN • Radio 2 - 5 GHz WLAN Note: Requires *FOUR, 5G-band* antennas connected to ANT sockets 1 to 4, and *FOUR, 5G-band* antennas connected to ANT sockets 5 to 8. Note: If using this mode, configure antenna-id for both group 1 and group 2 antennas.	5 GHz	5 GHz

Supported in the following platform

- Access Point — AP510e

Syntax

```
antenna-id external [group-1|group-2] <ANTENNA-TYPE>
```

Parameters

```
antenna-id external [group-1|group-2] <ANTENNA-TYPE>
```

antenna-id	Selects the antenna group to use and enables the access point radio.
external	States the antenna is external

group-1	Configures the antenna type used in the group-1 antenna ports (1 to 4). Note: Group-1 antenna configuration is required for all three software modes. Note: Refer to the table above for the supported software modes and the corresponding antenna configurations.
group-2	Configures the antenna type used in the group-2 antenna ports (5 to 8). Note: Group-2 antenna configuration is ONLY required for software modes 2 & 3. Note: Refer to the table above for the supported software modes and the corresponding antenna configurations.
antenna-type	Configures the antenna type used The antenna types supported for 'group-1' and 'group-2' antenna ports are: **ai-dq04360s**, **ml-2452-apa2-01**, **ml-2452-apa2-02**, **ml-2452-hpa5-036**, **ml-2452-hpag4a6-01**, **ml-2452-hpag5a8-01**, **ml-2452-pna5-01r**, **ml-2452-pna7-01r**, **ml-2452-pta4m4-036**, **ml-2452-sec6m4-036**, **ws-ai-dq05120**. By default *no* antenna-type is associated with the grouo-1 and group-2 antenna ports and the radio is disabled.

Usage Guidelines:

Following is the supported software modes for the AP510e access point radios:

Software Mode 1	• Radio 1: Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths • Radio 2: Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 2	• Radio 1: Set to 2.4/5 GHz Sensor • Radio 2: Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 3	• Radio 1: Set to 5 GHz, Channels 36 - 64 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths • Radio 2: Set to 5 GHz, Channels 100 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths

Example

```
ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#antenna-id ?
  group-1  Configure the antenna id on antenna group 1 (2.4/5GHz dual band
           antenna)
  group-2  Configure the antenna id on antenna group 2 (5GHz single band
           antenna)

ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#
ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#antenna-id group-1 ?
  ai-dq04360s         AI-DQ04360S Dual Band, Four Input Omni, 36 Inch Cable
  default             Internal antenna for internal SKU, no antenna for
                      external SKU
```

```
  ml-2452-apa2-01     ML-2452-APA2-01 3dBi/4.85dBi, dual band, black
  ml-2452-apa2-02     ML-2452-APA2-02 3dBi/4.85dBi, dual band, white
  ml-2452-hpa5-036    ML-2452-HPA5-036 3dBi/5dBi, dual band, outdoor, white
  ml-2452-hpag4a6-01  ML-2452-HPAG4A6-01 4dBi/7.3dBi, N-type male, dual band,
                      outdoor, white
  ml-2452-hpag5a8-01  ML-2452-HPAG5A8-01
  ml-2452-pna5-01r    ML-2452-PNA5-01R 2.4/5 GHz, Outdoor, Panel, 5 dBi, Beam
                      Width: E-Plane: 65 degrees, H-Plane: 120 degrees
  ml-2452-pna7-01r    ML-2452-PNA7-01R 8/12dBi 68deg Panel
  ml-2452-pta4m4-036  ML-2452-PTA4M4-036 4dBi/5 dBi, 4 port, dual band
  ml-2452-sec6m4-036  ML-2452-SEC6M4-036 DUAL POLARIZED DUAL BAND WIDE BEAM
                      DIRECTIONAL ANTENNA WITH 36 INCH CABLE
  ws-ai-dq05120       WS-AI-DQ05120 DUAL POLARIZED DUAL BAND WIDE BEAM
                      DIRECTIONAL ANTENNA WITH 36 INCH CABLE

ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#
ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#antenna-id group-2 ai-dq04360s
ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#show context
ap510 94-9B-2C-13-3C-9B
 use profile default-ap510
 use rf-domain default
 hostname ap510-133C9B
 no mint mlcp vlan
 no mint mlcp ip
 antenna-id group-1 ai-dq04360s
 interface radio1
 interface vlan1
  description "Virtual Interface for LAN by Wizard"
  ip address 192.162.4.159/24
  ip address zeroconf secondary
  no ip dhcp client request options all
 no virtual-controller
 no rf-domain-manager capable
 no adoption-mode
ap510-133C9B(config-device-94-9B-2C-13-3C-9B)#
```

Related Commands

no on page 1214	Removes the antenna-id configuration on the selected AP510e profile and device.

antenna-id (ap560h)

Profile Config Commands on page 853

Configures the antenna ID on an AP560h model access point profile and device. This command allows you to select the internal antenna modes.

The ExtremeMobility AP560h access point is a dual-radio access point, with eight, internal Wi-Fi antennas, supporting two internal antenna modes: *30 degree* and *70 degree*.

To enable the AP560h radio, configure the country code, map a WLAN to the radio, and configure the internal antenna mode as '30 degree' or '70 degree'.

Supported in the following platform

- Access Point — AP560h

Syntax

```
antenna-id internal [internal-560h-30|internal-560h-70|default]
```

Parameters

```
antenna-id internal [internal-560h-30|internal-560h-70|default]
```

antenna-id	Allows you to configure the functional mode for the AP560h access point's internal antennas.
internal	States the antenna is internal.
internal-560h-30	Configures the internal antenna mode as 30 degree.
internal-560h-70	Configure the internal antenna mode as 70 degree.
default	Sets the antenna mode to default. In this mode, *no* the antenna-mode is not specified and the radio is disabled. You must set the antenna mode to either 30 degree or 70 degree to turn-on the radios.

Radio Modes Supported

The AP560h supports the following radio modes:

Software Mode 1	• Radio 1: Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths • Radio 2: Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 2	• Radio 1: Set to 2.4/5 GHz Sensor • Radio 2: Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 3	• Radio 1: Set to 5 GHz, Channels 36 - 64 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths • Radio 2: Set to 5 GHz, Channels 100 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths

Example

```
nx9500-6C8809(config-profile-ap560h)#antenna-id internal internal-560h-70
nx9500-6C8809(config-profile-ap560h)#show context include-factory | include antenna-id
 antenna-id external group-1 default
 antenna-id external group-2 default
 antenna-id internal internal-560h-70
nx9500-6C8809(config-profile-ap560h)#
```

Related Commands

no on page 1214	Reverts the antenna mode to default on the selected AP560h profile and device.

alias

Profile Config Commands on page 853

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 172 (global config mode).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|igp|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 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.
	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. • <ADDRESS-RANGE-ALIAS-NAME> – Specify the address range alias name. Note: Alias name should begin with '$'.
<STARTING-IP> to <ENDING-IP>	Associates a range of IP addresses with this address range alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. 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.

```
alias encrypted-string <ENCRYPTED-STRING-ALIAS-NAME> <LINE>
```

encrypted-string <ENCRYPTED-STRING-ALIAS-NAME>	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 snmp-server on page 1539 (management policy config mode). • <ENCRYPTED-STRING-ALIAS-NAME> – Specify the encrypted-string alias name. Alias name should begin with '$'.

<LINE>	Configures the value associated with the alias name specified in the previous step
	• <LINE> – Configures the alias value
	Note: If password-encryption is enabled, in the `show > running-config` output, this clear text is displayed as an encrypted string, as shown below:
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`alias encrypted-string $enString 2`
	`fABMK2is7UToNiZE3MQXbgAAAAxB0ZIysdqsEJwr6AH/Da//`
	`!`
	`--More--`
	`nx9500-6C8809`
	`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:`
	`nx9500-6C8809(config)#show running-config`
	`!.............................`
	`!`
	`alias encrypted-string $enString 0 test11223344`
	`!`
	`--More--`
	`nx9500-6C8809`
	For more information on enabling password-encryption, see password-encryption on page 427.

```
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 1534 (management-policy mode). • <HASHED-STRING-ALIAS-NAME> – Specify the hashed-string alias name. 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/l/BXm9c4SBDv`
	`!`
	`alias hashed-string $PriMode 1`
	`faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112e`
	`cfc75`
	`--More--`
	`nx9500-6C8809`
	In the above `show > running-config` output, the '1' 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 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. • <HOST-ALIAS-NAME> – Specify the host alias name. Alias name should begin with '$'.
<HOST-IP>	Associates the network host's IP address with this host alias • <HOST-IP> – Specify the network host's IP address. 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.

```
alias network <NETWORK-ALIAS-NAME> <NETWORK-ADDRESS/MASK>
```

network <NETWORK-ALIAS-NAME>	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. 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-ALIAS-NAME> – Specify the network alias name. Alias name should begin with '$'.
<NETWORK-ADDRESS/MASK>	Associates a single network with this network alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. 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.

```
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>	Creates a new network-group alias for this profile. Or associates an existing network-group alias with this profile. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name. Alias name should begin with '$'. 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. After specifying the name, specify the following: a range of IP addresses, host addresses, or a range of network addresses. 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.
address-range <STARTING-IP> to <ENDING-IP> {<STARTING-IP> to <ENDING-IP>}	Associates a range of IP addresses with this network-group alias • <STARTING-IP> – Specify the first IP address in the range. • to <ENDING-IP> – Specify the last IP address in the range. <STARTING-IP> to <ENDING-IP> – Optional. Specifies more than one range of IP addresses. A maximum of eight (8) IP address ranges can be configured.

host <HOST-IP> {<HOST-IP>}	Associates a single or multiple hosts with this network-group alias • <HOST-IP> – Specify the host's IP address. • <HOST-IP> – Optional. Specifies more than one host. A maximum of eight (8) hosts can be configured.
network <NETWORK-ADDRESS/MASK> {<NETWORK-ADDRESS/MASK>}	Associates a single or multiple networks with this network-group alias • <NETWORK-ADDRESS/MASK> – Specify the network's address and mask. • <NETWORK-ADDRESS/MASK> – Optional. Specifies more than one network. A maximum of eight (8) networks can be configured.

```
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)}
```

alias network-service <NETWORK-SERVICE-ALIAS-NAME>	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. <NETWORK-SERVICE-ALIAS-NAME> – Specify a network-service alias name. Note: Alias name should begin with '$'. 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. Note: 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.
proto [<0-254>| <WORD>|eigrp|gre| igmp|igp|ospf|vrrp]	Use one of the following options to associate an Internet protocol with this network-service alias: • <0-254> – 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. • <WORD> – Identifies the protocol by its name. Specify the protocol name. • eigrp – Selects EIGRP *(Enhanced Interior Gateway Routing Protocol)*. The protocol number 88. • gre – Selects GRE *(Generic Routing Encapsulation)*. The protocol number is 47. • igmp – Selects IGMP *(Internet Group Management Protocol)*. The protocol number is 2. • igp – Selects IGP *(Interior Gateway Protocol)*. The protocol number is 9. • ospf – Selects OSPF *(Open Shortest Path First)*. The protocol number is 89. • vrrp – Selects VRRP *(Virtual Router Redundancy Protocol)*. The protocol number is 112.
{(<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)}	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. • <1-65535> – Optional. Configures a destination port number from 1 - 65535 • <WORD> – Optional. Identifies the destination port by the service name provided. For example, the SSH *(secure shell)* service uses TCP port 22. • bgp – Optional. Configures the default BGP *(Border Gateway Protocol)* services port (179) • dns – Optional. Configures the default DNS *(Domain Name System)* services port (53) • ftp – Optional. Configures the default FTP *(File Transfer Protocol)* control services port (21)

	• ldap – Optional. Configures the default LDAP *(Lightweight Directory Access Protocol)* services port (389)
	• ftp-data – Optional. Configures the default FTP data services port (20)
	• gopher – Optional. Configures the default gopher services port (70)
	• https – Optional. Configures the default HTTPS services port (443)
	• nntp – Optional. Configures the default Newsgroup (NNTP) services port (119)
	• ntp – Optional. Configures the default NTP *(Network Time Protocol)* services port (123)
	• 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).
	• 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 exmple, • The number alias name is: $NUMBER • The value assigned is: 100 The value d by alias $NUMBER, wherever used, is 100. • <NUMBER-ALIAS-NAME> – Specify the number alias name. • <0-4294967295> – Specify the number, from 0 - 4294967295, assigned to the number alias created. Note: Alias name should begin with '$'.

```
alias string <STRING-ALIAS-NAME> <LINE>
```

alias string <STRING-ALIAS-NAME>	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. • <STRING-ALIAS-NAME> – Specify the string alias name. • <LINE> – Specify the string value. Note: Alias name should begin with '$'. 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.

```
alias vlan <VLAN-ALIAS-NAME> <1-4094>
```

alias vlan <VLAN-ALIAS-NAME>	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. 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. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name. Note: Alias name should begin with '$'.
<1-4094>	Maps the VLAN alias to a VLAN ID • <1-4094> – Specify the VLAN ID from 1 - 4094. 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.

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 proto 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
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
alias network-service $kerberos proto tcp 88 proto udp 389
nx9500-6C8809(config-profile-testRFS4k)#
```

Related Commands

no on page 1214	Removes a specified alias configuration

application-policy

Profile Config Commands on page 853

Associates a RADIUS server provided 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 195.

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
application-policy radius <APP-POLICY-NAME>
```

Parameters

```
application-policy radius <APP-POLICY-NAME>
```

application-policy radius <APP-POLICY-NAME>	Associates a RADIUS server provided application policy with this profile • <APP-POLICY-NAME> – Specify the application policy name (should be existing and configured).

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

no on page 1214	Removes the RADIUS-server provided application policy associated with this profile

area

Profile Config Commands on page 853

Sets the system's area of location (the physical area of deployment)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
area <WORD>
```

Parameters

```
area <WORD>
```

area <WORD>	Sets the system's area of location • <WORD> – Specify the area name (should not exceed 64 characters).

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 me1
 interface ge1
--More--
nx9500-6C8809(config-profile-default-rfs4000)#
```

Related Commands

no on page 1214	Resets the configured area name

arp

Profile Config Commands on page 853

Adds a static ARP *(Address Resolution Protocol)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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}
```

arp <IP>	Adds a static ARP IPv4 address in the ARP cache • <IP> – Specify the static IP address.
<MAC>	Specify the MAC address associated with the IP and the Switch Virtual Interface (SVI).
arpa	Sets ARP encapsulation type to ARPA
<L3-INTERFACE-NAME>	Configures static ARP entry for a specified router interface • <L3-INTERFACE-NAME> – Specify the router interface name.
pppoe1	Configures static ARP entry for PPP over Ethernet interface
vlan <1-4094>	Configures static ARP entry for a VLAN interface • <1-4094> – Specify a SVI VLAN ID from 1 - 4094.
wwan1	Configures static ARP entry for Wireless WAN interface
{dhcp-server|router}	The following keywords are common to all off the above interface types: • dhcp-server – Optional. Sets ARP entries for a DHCP server • router – Optional. Sets ARP entries for a router

```
arp timeout <15-86400>
```

arp timeout <15-86400>	Sets ARP entry timeout • <TIME> – Sets the ARP entry timeout in seconds. Specify a value from 15 - 86400 seconds. The default is 3600 seconds.

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

no on page 1214	Removes an entry from the ARP cache

auto-learn

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
auto-learn [host-name-via-dhcp <WORD>|staging-config]
```

Parameters

```
auto-learn [host-name-via-dhcp <WORD>|staging-config]
```

auto-learn [host-name-via-dhcp <WORD>| staging-config]	Enables auto-learning of: • host-name-via-dhcp – A device's host name via DHCP option. • <WORD> – 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. • 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

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

no on page 1214	Disables automatic recognition of devices' hostname and devices pending adoption

autogen-uniqueid

Profile Config Commands on page 853

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 – TestAP505
- substitution token – $SN

The unique ID is generated using TestAP505$SN, where $SN is replaced with the device's serial number.

When executed on an AP505 (having serial number 1902W-2013400000), the autogen-uniqueid TestAP505$SN command generates the unique ID: TestAP5051902W-2013400000. When configured on an AP505 profile, all AP505s using the profile auto-generate a unique ID in which the device's serial number is preceded by the string 'TestAP505'.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 ap505 ap510
 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 1214	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 853

Automatically installs firmware image and startup configuration parameters on to the selected device.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

Parameters

```
autoinstall [configuration|firmware|start-interval <WORD>]
```

configuration	Autoinstalls startup configuration. Setup parameters are automatically configured on devices using this profile. This option is disabled by default.
firmware	Autoinstalls firmware image. Firmware images are automatically installed on devices using this profile. This option is disabled by default.
start-interval <WORD>	Configures the interval between system boot and start of autoinstall process (this is the time, from system boot, after which autoinstall should start) • <WORD> – Specify the interval in minutes. The default is 10 minutes. **Note:** Zero (0) implies firmware or startup configuration installation can start any time.

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

no on page 1214	Disables the auto install settings

bridge

Configures VLAN Ethernet bridging parameters. Use this command to configure a Bridge NAT or Bridge VLAN settings

Configuring bridge NAT *(Network Address Translation)* 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 VLAN *(Virtual LAN)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>|wwan1]
[(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>)]
```

nat	Configures bridge NAT parameters
source	Configures NAT source addresses

list <IP-ACCESS-LIST-NAME> precedence <1-500>	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. • <IP-ACCESS-LIST-NAME> – Specify access list name. • precedence <1-500> – Specifies a precedence value for this bridge NAT policy.
interface [<LAYER3-INTERFACE-NAME>| pppoe1|vlan <1-4094>| wwan1]	Selects one of the following as the primary interface (between the source and destination points): • <LAYER3-INTERFACE-NAME> – A router interface. Specify interface name. • pppoe1 – A PPP over Ethernet interface. • vlan <1-4094> – A VLAN interface. Specify the VLAN interface index from 1 - 4094. • wwan1 – A Wireless WAN interface.
[(address|interface| overload|pool <NAT-POOL-NAME>)]	The following keywords are recursive and common to all interface types: • address – Configures the interface IP address used for NAT • interface – Configures the failover interface (default setting) • overload – Enables use of one global address for multiple local addresses (terminates command) • pool <NAT-POOLNAME> – Configures the NAT pool used with this bridge NAT policy. Specify the NAT pool name. For more information on configuring a NAT pool, see nat-pool-config-instance on page 1173.

```
bridge vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

vlan <1-4094>	Configures the numerical identifier for the Bridge VLAN when it was initially created. • <1-4094> – Specify a VLAN index from 1 - 4094.
vlan <VLAN-ALIAS-NAME>	Configures the VLAN alias (should be existing and configured) identifying the bridge VLAN • <VLAN-ALIAS-NAME> – Specify a VLAN alias name.

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

The following table summarizes bridge VLAN configuration mode commands:

Table 35: Bridge VLAN Config Mode Commands

Command	Description
bridging-mode on page 886	Configures how packets on this VLAN are bridged
captive-portal on page 887	Enables IP packet snooping on wired captive portals, and also configures the subnet to snoop
captive-portal-enforcement on page 888	Enables auto-enforcement of captive portal rules on this extended VLAN interface
description on page 889	Configures VLAN bridge description
edge-vlan on page 890	Enables edge VLAN mode

Table 35: Bridge VLAN Config Mode Commands (continued)

Command	Description
firewall on page 890	Enables firewall on this bridge VLAN interface
http-analyze on page 891	Enables the analysis of URLs and data traffic on this Bridge VLAN
ip on page 891	Configures IP components
ipv6 on page 895	Configures IPv6 components
l2-tunnel-broadcast-optimization on page 897	Enables broadcast optimization
l2-tunnel-forward-additional-packet-types on page 898	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.
mac-auth on page 899	Enables MAC authentication for Extended VLAN and Tunneled traffic (both MiNT and L2TPv3)
name on page 900	Configures a name for the selected Bridge VLAN
no on page 906	Negates a command or reverts settings to their default
stateful-packet-inspection-l2 on page 903	Enables stateful packet inspection in the layer 2 fire wall
registration on page 901	Enables forwarding of bridge-vlan information (such as, name and vlan) to the ExtremeGuest (EGuest) server.
tunnel on page 904	Enables tunneling of unicast messages to unknown MAC destinations, on the selected VLAN bridge
tunnel-over-level2 on page 905	Enables extended VLAN traffic over level 2 MiNT links
use on page 908	Associates a captive-portal, access control list (IP, IPv6, or MAC), and a URL filter with this bridge VLAN

bridging-mode

bridge on page 883

Configures how packets are bridged on the selected VLAN

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

Parameters

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

bridging-mode	Configures the VLAN bridging mode
auto	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)

isolated-tunnel	Bridges packets between local Ethernet ports and local radios, and passes tunneled packets through without de-tunneling Select this option for a dedicated tunnel for bridging VLAN traffic.
local	Bridges packets normally between local Ethernet ports and local radios (if any) 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.
tunnel	Bridges packets between local Ethernet ports, local radios, and tunnels to other APs, wireless controllers, or service platforms Select this option to use a shared tunnel for bridging VLAN traffic. 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

no on page 906	Resets bridging mode to auto

captive-portal

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>}
```

captive-portal [ipv4-snooping| ipv6-snooping]	Enables snooping of IPv4 or IPv6 packets (based on the option selected) for wired captive portal clients
subnet <IPv4/M| IPv6/M>	Enables IPv4 or IPv6 packet snooping on a specified subnet • <IPv4/M|IPv6/M> – Specify the subnet address in the A.B.C.D/M or X: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.
excluded-address <IPv4|IPv6>	Optional. Configures the IPv4 or IPv6 address excluded from snooping within the specified IPv4|IPv6 subnet. • <IPv4|IPv6> – Specify the IPv4 or IPv6 address. Use this parameter to configure the gateway's address.

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

no on page 906	Disables IP packet snooping on wired captive portals

captive-portal-enforcement

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fallback}
```

captive-portal-enforcement	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. 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.
fall-back	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

no on page 906	Disables auto-enforcement of captive portal rules on this extended VLAN interface

description

bridge on page 883

Configures this extended VLAN's description

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this VLAN bridge • <WORD> – Enter a description. The description should be unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.

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

no on page 906	Removes VLAN's description

edge-vlan

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 906	Disables the edge VLAN mode

firewall

bridge on page 883

Enables IPv4 firewall on this Bridge VLAN. This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 906	Disables firewall on this bridge VLAN interface

http-analyze

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
http-analyze {filter [images|post|query-string]}
```

Parameters

```
http-analyze {filter [images|post|query-string]}
```

http-analyze filter [images|post|query-string]	Enables URL and HTTP data analysis. Optionally use the filter keyword to filter out specific URLs
	• filter – Optional. Filters out specific URLs
	  • images – Filters out URLs referring to images
	  • post – Filters out URLs referring to POSTs
	  • query-string – Filters out query strings received from URLs

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

no on page 906	Disables forwarding of URLs and data to the controller running the HTTP analytics engine

ip

bridge on page 883

Configures this Bridge VLAN's IP components

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, 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
```

ip	Configures the VLAN bridge IP parameters
arp trust	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. • trust – Trusts ARP responses on the VLAN bridge
dhcp trust	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. • trust – Trusts DHCP responses on the VLAN bridge

```
ip igmp snooping {fast-leave|forward-unknown-multicast|last-member-query-count <1-7>}
```

ip	Configures the VLAN bridge IP parameters
igmp snooping	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.
fast-leave	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.

forward-unknown-multicast	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.
last-member-query-count <1-7>	Optional. Configures the last member query count used in determining the number of group-specific queries sent before removing the snoop entry • <1-7> – Specify the count from 1 - 7. The default value is 2.

```
ip igmp snooping {mrouter [interface <INTERFACE-LIST>|learn pim-dvmrp]}
```

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures the IGMP snooping parameters
mrouter	Optional. Configures the multicast router parameters
interface <INTERFACE-LIST>	Configures the multicast router interfaces. This option is disabled by default. • <INTERFACE-LIST> – Specify a comma-separated list of interface names.
learn pim-dvmrp	Configures the multicast router learning protocols. This option is disabled by default. • pim-dvmrp – Enables Protocol-Independent Multicast (PIM) and Distance-Vector Multicast Routing Protocol (DVMRP) snooping of packets

```
ip igmp snooping {querier} {address <IP>|max-response-time <1-25>| timer expiry <60-300>|
version <1-3>}
```

ip	Configures the VLAN bridge IP parameters
igmp snooping	Configures the IGMP snooping parameters
querier	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.
address <IP>	Optional. Configures the IGMP querier source IP address. This address is used as the default VLAN querier IP address. • <IP> – Specify the IGMP querier source IP address.

max-response-time <1-25>	Optional. Configures the IGMP querier maximum response time. This option is disabled by default. • <1-25> – Specify the maximum response time from 1 - 25 seconds. 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. If no reports are received from a radio, it is removed from the snooping table. The radio then stops receiving multicast packets.
timer expiry <60-300>	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. • expiry – Configures the IGMP querier timeout • <60-300> – Specify the IGMP querier timeout from 60 - 300 seconds.
version <1-3>	Optional. Configures the IGMP version. This option is disabled by default. • <1-3> – Specify the IGMP version. The versions are 1- 3.

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 906	Disables or reverts the VLAN Ethernet bridge parameters

ipv6

bridge on page 883

Configures this Bridge VLAN's IPv6 components

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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
```

ipv6	Configures the VLAN bridge IPv6 parameters
dhcpv6 trust	Enables the DHCPv6 trust option. When enabled all DHCPv6 responses are trusted on this bridge VLAN. This option is enabled by default. • trust – Trusts DHCPv6 responses on this bridge VLAN

```
ipv6 firewall
```

ipv6	Configures the VLAN bridge IPv6 parameters
firewall	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 ND *(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 such a request with a RA *(router advertisement)* packet that contains Internet layer configuration parameters.

```
ipv6 mld snooping {forward-unknown-multicast}
```

ipv6	Configures the VLAN bridge IPv6 parameters
mld snooping	Configures MLDP *(Multicast Listener Discovery Protocol)* 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.
forward-unknown-multicast	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]}
```

ipv6	Configures the VLAN bridge IPv6 parameters
mld snooping	Configures MLD snooping parameters. This option is enabled by default.
mrouter	Optional. Configures the multicast router parameters, such as interfaces and learning protocol used.
interface <INTERFACE-LIST>	Configures the multicast router interfaces. This option is disabled by default. • <INTERFACE-LIST> – Specify a comma-separated list of interface names.
learn pim-dvmrp	Configures the multicast router learning protocols. This option is disabled by default. • pim-dvmrp – Enables PIM and DVMRP snooping of packets

```
ipv6 mld snooping {querier} {max-response-time <1-25000>|timer expiry <60-300>| version
<1-2>}
```

ipv6	Configures the VLAN bridge IPv6 parameters
mld snooping	Configures IPv6 MLD snooping parameters. This option is disabled by default.
querier	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.
max-response-time <1-25000>	Optional. Configures the IPv6 MLD querier's maximum response time. This option is disabled by default. • <1-25000> – Specify the maximum response time from 1 - 25000 milliseconds.

timer expiry <60-300>	Optional. Configures the IPv6 MLD other querier's timeout. This option is disabled by default. • <60-300> – Specify the MLD other querier's timeout from 60 - 300 seconds.
version <1-2>	Optional. Configures the IPv6 MLD querier version. This option is disabled by default. • <1-2> – Specify the MLD version. The versions are 1- 2.

```
ipv6 nd raguard
```

ipv6	Configures the VLAN bridge IPv6 parameters
nd raguard	Allows 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

no on page 906	Disables or reverts the VLAN Ethernet bridge IPV6 parameters

l2-tunnel-broadcast-optimization

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 906	Disables L2 tunnel broadcast optimization

l2-tunnel-forward-additional-packet-types

bridge on page 883

Enables forwarding of WNMP *(Wireless Network Management Protocol)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 906	Disables WNMP packet forwarding across L2 tunnel

mac-auth

bridge on page 883

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, NX9500, NX9600, VX9000

Syntax

```
mac-auth {attempts <1-5>|throttle <0-255>}
```

Parameters

```
mac-auth {attempts <1-5>|throttle <0-255>}]
```

mac-auth	Enables MAC Authentication
attempts <1-5>	Optional. Configures the maximum number of retries allowed for MAC authentication requests. • <1-5> – Specify the maximum allowed authentication retries from 1 - 5. The default is 3.
throttle <0-255>	Optional. Configures the throttle value for MAC authentication requests • <0-255> – Specify the MAC authentication request throttle value from 0 -255. The default is 64.

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

no on page 906	Disables MAC authentication for Extended VLAN and Tunneled traffic on this bridge VLAN

name

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
name <NAME>
```

Parameters

```
name <NAME>
```

name <NAME>	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

no on page 906	Removes or modifies this Bridge VLANs configured name

registration

bridge on page 883

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 900.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
registration [device|device-OTP|external|user]
registration [device|device-OTP|user] group-name <RAD-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>}
```

registration	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.
[device|device-OTP| user]	Configures the mode used to register wired clients on this bridge-vlan interface. The options are: device, user, and device-OTP. • 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. • device – Registers device by its MAC address, and allows access to already registered clients. Note: If using the above two options, ensure MAC authentication is enabled on the bridge-vlan interface. • user – Registers guest users using one of the following options: e-mail address, mobile-number, or member-id. 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.
group-name <RAD-GROUP-NAME>	Configures the RADIUS group name in which registered users are placed. When left blank, users are not associated with a RADIUS group. • <RAD-GROUP-NAME> – Specify the RADIUS group name (should not exceed 64 characters).
expiry-time <1-43800>	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. • <1-43800> – Specify a value from 1 - 43800 hrs. The default is 1500 hrs.

```
registration external follow-aaa send-mode [http|https|udp]
```

registration	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.
external	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.

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. This is the AAA policy used in the captive-portal applied on the bridge-vlan interface. 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. For more information on enabling the EGuest server, see eguest-server (VX9000 only) on page 987 (profile config mode).
send-mode [https|https|udp]	Specifies the protocol used to forward registration requests to the external AAA policy server. The options are: • HTTPS – Sends registration requests as HTTPS packet • HTTP – Sends registration requests as HTTP packet • UDP – Sends registration requests as UDP packet. This is the default setting.

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

no on page 906	Disables self-registration of captive-portal users on this bridge-vlan interface.

stateful-packet-inspection-l2

bridge on page 883

Enables a SIP *(stateful packet inspection)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
stateful-packet-inspection-l2
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#stateful-packet-ins
inspection-l2
nx9500-6C8809(config-profile-default-rfs4000-bridge-vlan-1)#
```

Related Commands

no on page 906	Disables stateful packet inspection at the layer 2 firewall

tunnel

bridge on page 883

Enables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 906	Disables tunneling of unicast messages, to unknown MAC destinations, on the selected VLAN bridge

tunnel-over-level2

bridge on page 883

Enables extended VLAN (tunneled VLAN) traffic over level 2 MiNT links. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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"
  l2-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

no on page 906	Disables extended VLAN traffic over level 2 MiNT links

no

bridge on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [bridging-mode|captive-portal|captive-portal-enforcement|description|edge-vlan|
firewall|http-analyze|ip|ipv6|l2-tunnel-broadcast-optimization|l2-tunnel-forward-
```

```
additional-packet-types|mac-auth|name|registration|stateful-packet-inspection-l2|tunnel|
tunnel-over-level2|use]

no [bridging-mode|captive-portal-enforcement|description|edge-vlan|firewall|l2-tunnel-
broadcast-optimization|l2-tunnel-forward-additional-packet-types| mac-auth|name|stateful-
packet-inspection-l2|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 raguard

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>
```

no <PARAMETERS>	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 on page 883

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use [application-policy|captive-portal|ip-access-list|ipv6-access-list|mac-access-list|
purview-application-policy|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>

use purview-application-policy <PURVIEW-APP-POLICY-NAME>
```

Parameters

```
use application-policy <APP-POLICY-NAME>
```

use application-policy <APP-POLICY-NAME>	Enforces application detection on this VLAN bridge • <APP-POLICY-NAME> – Specify the application policy name (should be existing and configured). • For more information on application definitions and application policy, see application on page 183 and application-policy on page 195.

```
use captive-portal <CAPTIVE-PORTAL-NAME>
```

use captive-portal	Applies an existing captive portal configuration to restrict access to the bridge VLAN configuration 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. • <CAPTIVE-PORTAL-NAME> – Specify the captive portal name.

```
use [ip-access-list|ipv6-access-list|mac-access-list] tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>
```

use	Sets this VLAN bridge policy to use an IPv4/IPv6 access list or a MAC access list
ip-access-list	Associates a pre-configured IPv4 access list with this VLAN-bridge interface
ipv6-access-list	Associates a pre-configured IPv6 access list with this VLAN-bridge interface
mac-access-list	Associates a pre-configured MAC access list with this VLAN- bridge interface
tunnel out <IP/IPv6/MAC-ACCESS-LIST-NAME>	The following keywords are common to the 'IPv4/IPv6 access list' and 'MAC access list' parameters: • tunnel – Applies IPv4/IPv6 access list or MAC access list to all packets going into the tunnel • out – Applies IPv4/IPv6 access list or MAC access list to all outgoing packets <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the IP/IPv6 access list or MAC access list name.

```
use url-filter <URL-FILTER-NAME>
```

use url-filter	Sets this VLAN bridge to use a URL filter
<URL-FILTER-NAME>	Specify the URL filter name. It should be existing and configured. This option enforces URL filtering on the VLAN bridge.

```
use purview-application-policy <PURVIEW-APP-POLICY-NAME>
```

use purview-application-policy <PURVIEW-APP-POLICY-NAME>	Enforces application detection on this VLAN bridge • <PURVIEW-APP-POLICY-NAME> – Specify the Purview application policy name (should be existing and configured). Note: *EAA (Extreme Application Analytics)* (Purview™) is supported only on the WiNG 7.1.2 APs. Note: For information on Purview application policy, see purview-application-policy on page 436.

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

no on page 906	Disables or reverts VLAN Ethernet bridge settings

captive-portal

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
captive-portal page-upload count <1-20>
```

Parameters

```
captive-portal page-upload count <1-20>
```

page-upload	Enables captive portal advanced Web page upload
count <1-20>	Sets the maximum number of APs that can be uploaded concurrently • <1-20> – Set a value from 1 - 20. The default is 10.

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)#
```

cdp

Profile Config Commands on page 853

Enables CDP *(Cisco Discovery Protocol)*, 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cdp [holdtime|run|timer]
cdp [holdtime <10-1800>|run|timer <5-900>]
```

Parameters

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

holdtime <10-1800>	Specifies the holdtime after which transmitted packets are discarded • <10-1800> – Specify a value from 10 - 1800 seconds. The default is 180 seconds.
run	Enables CDP sniffing and transmit globally. This feature is enabled by default.
timer <5-900>	Specifies the interval, in seconds, between successive CDP packet transmission • <5-900> – Specify a value from 5 - 900 seconds. The default is 60 seconds.

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 802.1p
 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

no on page 1214	Disables CDP on this profile

cluster

Profile Config Commands on page 853

Sets the cluster configuration

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

force-configured-state	Forces adopted APs to auto revert when a failed wireless controller or service platform (in a cluster) restarts 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. This feature is disabled by default.
force-configured-state-delay <3-1800>	Forces cluster transition to the configured state after a specified interval • <3-1800> – Specify a delay from 3 - 1800 minutes. The default is 5 minutes. This is the interval a standby controller waits before releasing adopted APs when a failed primary controller becomes active again.

handle-stp	Enables STP *(Spanning Tree Protocol)* convergence handling. This feature is disabled by default. 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.
master-priority <1-255>	Configures cluster master priority • <1-255> – Specifies cluster master election priority. Assign a value from 1 - 255. Higher the value higher is the precedence. The default is 128. 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.

```
cluster member [ip <IP> {level [1|2]}|vlan <1-4094>]
```

member	Adds a member to the cluster. It also configures the cluster VLAN where members can be reached.
ip <IP> level [1|2]	Adds IP address of the new cluster member • <IP> – Specify the IP address. • level – Optional. Configures routing level for the new member. Select one of the following routing levels: 1 – Level 1, local routing 2 – Level 2, In-site routing
vlan <1-4094>	Configures the cluster VLAN where members can be reached • <1-4094> – Specify the VLAN ID from 1- 4094.

```
cluster mode [active|standby]
```

mode [active|standby]	Configures cluster member's mode as active or standby • active – Configures cluster mode as active. This is the default setting. • standby – Configures cluster mode as standby 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.

```
cluster name <CLUSTER-NAME>
```

name <CLUSTER-NAME>	Configures the cluster name • <CLUSTER-NAME> – Specify the cluster name.

```
cluster radius-counter-db-sync-time <1-1440>
```

radius-counter-db-sync-time <1-1440>	Configures the interval, in minutes, at which the RADIUS counter database is synchronized with the dedicated NTP server resource. • <1-1440> – Specify a value from 1 - 1440 minutes. The default is 5 minutes. Use the `show > cluster > configuration` 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

no on page 1214	Removes cluster member

configuration-persistence

Profile Config Commands on page 853

Enables configuration persistence across reloads. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
configuration-persistence {auto|secure}
```

Parameters

```
configuration-persistence {auto|secure}
```

auto	Optional. Assigns default value based on the device type
secure	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

no on page 1214	Disables automatic write up of startup configuration file

controller

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
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]
```

controller	Configures the WLAN's controller adoption settings
adopted-devices	Configures the types of device (AP/controller) this controller can adopt
aps {controllers}	Enables the adoption of network access points by this controller. This option is enabled by default. • controllers – Optional. Enables the adoption of peer controllers by this controller All adopted devices (referred to as adoptee) receive complete configuration from the adopting controller (referred to as adopter).
controllers {aps}	Enables the adoption of peer controllers by this controllers • aps – Optional. Enables the adoption of network access points by this controller 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. Use the `no > controller > adopted-devices` command to remove this setting.
external-devices	Enables adoption of external devices by this controller. This option is disabled by default. 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. To disable T5 or EX3500 adoption, use the no > controller > external-devices command. This feature is supported only on RFS4000, NX9500, NX9510, NX9600, and VX9000 platforms.
external-devices-monitoring-only	Enables only monitoring of external devices by this controller or service platform. This option is disabled by default.

```
controller adoption
```

controller adoption	Enables the adoption of the logged device (wireless controller or service platform) by other controllers. This option is disabled by default. Use the `no > controller > adoption` command to disable adoption.

```
controller [group <CONTROLLER-GROUP-NAME>|vlan <1-4094>]
```

controller	Configures the WLAN's controller adoption settings
group <CONTROLLER-GROUP-NAME>	Configures the wireless controller or service platform group • <CONTROLLER-GROUP-NAME> – Specify the wireless controller or service platform group name.
vlan <1-4094>	Configures the wireless controller or service platform VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094.

```
controller hello-interval <1-120> adjacency-hold-time <2-600>
```

controller	Configures the WLAN's controller settings
hello-interval <1-120>	Configures the hello-interval in seconds. This is the interval between consecutive hello packets exchanged between AP and wireless controller or service platform. • <1-120> – Specify a value from 1 - 120 seconds.
adjacency-hold-time <2-600>	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. • <2-600> – Specify a value from 2 - 600 seconds.

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {ipsec-secure} {gw [<IP>|<HOSTNAME>]}
```

controller	Configures the WLAN's controller adoption settings
host [<IPv4>|<IPv6>|<HOSTNAME>]	Configures wireless controller or service platform's IPv4/IPv6 address or hostname • <IPv4> – Configures wireless controller or service platform's IPv4 address • <IPv6> – Configures wireless controller or service platform's IPv6 address • <HOSTNAME> – Configures wireless controller or service platform's hostname

ipsec-secure {gw [<IP>|<HOSTNAME>]}	Optional. Enables Internet Protocol Security (IPSec) peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
	• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform
	  • <IP> – Use this option to specify the IPSec gateway's IP address.
	  • <HOSTNAME> – Use this option to specify the IPSec gateway's hostname.
	If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {level [1|2]|pool <1-2> level [1|2]} {ipsec-
secure {gw [<IP>|<HOSTNAME>]}|remote-vpn-client}
```

controller	Configures the WLAN's controller adoption settings
host [<IPv4>|<IPv6>|<HOSTNAME>]	Configures wireless controller or service platform's IPv4/IPv6 address or name • <IPv4> – Configures wireless controller or service platform's IPv4 address • <IPv6> – Configures wireless controller or service platform's IPv6 address • <HOSTNAME> – Configures wireless controller or service platform's name
level [1|2]	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: • 1 – Optional. Level 1, local routing • 2 – Optional. Level 2, inter-site routing Note: After specifying the routing level, you can, optionally enable IPSec Secure authentication and remote VPN client.

pool <1-2> level [1|2]	The following keywords are common to the 'IP', 'IPv6', and 'hostname' parameters:
	Optional. Sets the wireless controller or service platform's pool
	• <1-2> – 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:
	  • 1 – Optional. Level 1, local routing
	  • 2 – Optional. Level 2, inter-site routing

{ipsec-secure {gw [<IP>|<HOSTNAME>]}| remote-vpn-client}	After specifying the routing level and or device's pool, you can optionally specify the following:
	• ipsec-secure – Optional. Enables IPSec peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
	• gw – Optional. Specifies a IPSec gateway other than the wireless controller or service platform
	  • <IP> – Use this option to specify the IPSec gateway's IP address.
	  • <HOSTNAME> – Use this option to specify the IPSec gateway's hostname.
	
	  Note: If the gateway's IP address or hostname is not specified, the system assumes the logged controller as the IPSec gateway.
	• remote-vpn-client – Forces MiNT link creation protocol (MLCP) to use remote VPN connection on the controller
	
	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.

```
controller host [<IPv4>|<IPv6>|<HOSTNAME>] {remote-vpn-client}
```

controller	Configures the WLAN's controller settings
host [<IPv4>|<IPv6>|<HOSTNAME>]	Configures wireless controller or service platform's IPv4/IPv6 address or hostname • <IP> – Configures wireless controller or service platform's IPv4 address • <IPv6> – Configures wireless controller or service platform's IPv6 address • <HOSTNAME> – Configures wireless controller or service platform's name
remote-vpn-client	Forces MLCP to use remote VPN connection on the controller 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.

Example

```
nx9500-6C8809(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 1214	Disables or reverts settings to their default

critical-resource

Profile Config Commands on page 853

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 CRM *(critical resource monitoring)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]}}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor	Enables critical resource(s) monitoring

direct [all|any] [<IP/HOST-ALIAS-NAME>| sync-adoptees]	Monitors critical resources using the default routing engine • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable) • <IP/HOST-ALIAS-NAME> – 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. • 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.
arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>] {<IP/HOST-ALIAS-NAME>| port [<LAYER2-IFNAME>| ge| port-channel]}	The following keywords are common to the 'all' and 'any' parameters: • arp-only vlan <1-4094> – 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. • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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. <IP/HOST-ALIAS-NAME> – Optional. Limits ARP to a device specified by the <IP> 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. port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port

```
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]}}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor	Enables critical resource(s) monitoring
via	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.
<IP/HOST-ALIAS-NAME>	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.

<LAYER3-INTERFACE-NAME>	Specify the layer 3 Interface name (router interface)
pppoe1	Specifies PPP over Ethernet interface
vlan [<1-4094>|<VLAN-ALIAS-NAME>]	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.
wwan1	Specifies Wireless WAN interface
[all|any] [<IP/HOST-ALIAS-NAME>| sync-adoptees]	Monitors critical resources using the default routing engine • all – Monitors all resources that are going down (generates an event when all specified critical resource IP addresses are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource IP address is unreachable) • <IP/HOST-ALIAS-NAME> – 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. • 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.
arp-only vlan [<1-4094>|<VLAN-ALIAS-NAME>] {<IP/HOST-ALIAS-NAME>| port [<LAYER2-IFNAME>| ge| port-channel]}	The following keywords are common to the 'all' and 'any' parameters: • arp-only vlan <1-4094> – 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. • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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. • <IP'HOST-ALIAS-NAME> – Optional. Limits ARP to a device specified by the <IP> 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. • port [<LAYER2-IF-NAME>|ge|port-channel] – Optional. Limits ARP to a specified port

```
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>}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor-using-flows	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.

[all|any]	Configures how critical resource event messages are generated. Options include all and any. • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)
criteria [all|cluster-master| rf-domain-manager]	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. • all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource • cluster-master – Configures the cluster master as the monitoring resource • rf-domain-manager – Configures the RF Domain manager as the monitoring resource
dhcp vlan [<1-4094>| <VLAN-ALIAS-NAME>]	The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords: • 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. • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.

dns <IP/HOST-ALIAS-NAME>	The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords: • 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. • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

{dhcp [vlan <1-4094>| <VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>}	The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).
	• 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.
	  • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.
	• 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.
	  • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

```
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>}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor-using-flows	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.
[all|any]	Configures how critical resource event messages are generated. Options include all and any. • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)

dhcp vlan [<1-4094>| <VLAN-ALIAS-NAME>]	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. • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.

{dhcp vlan [<1-4094>| <VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>}	The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):
	• 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.
	  • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.
	• 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.
	  • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

```
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>}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor-using-flows	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.
[all|any]	Configures how critical resource event messages are generated. Options include all and any. • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)

dns <IP/HOST-ALIAS-NAME>	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. • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

{dhcp vlan [<1-4094>| <VLAN-ALIAS-NAME>| dns <IP/HOST-ALIAS-NAME>}	The following parameters are recursive and optional. Use them to configure multiple VLANs and critical resource IPv4 addresses (or host alias names):
	• 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.
	  • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.
	• 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.
	  • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

```
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>}
```

<CR-NAME>	Identifies the critical resource to be monitored. Provide the name of the critical resource.
monitor-using-flows	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.
[all|any]	Configures how critical resource event messages are generated. Options include all and any. • all – Monitors all resources that are going down (generates an event when all specified critical resources are unreachable) • any – Monitors any resource that is going down (generates an event when any one of the specified critical resource is unreachable)
syn-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.

criteria [all|cluster-master| rf-domain-manager]	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. • all – Configures all devices within a group (cluster or RF Domain) as the monitoring resource • cluster-master – Configures the cluster master as the monitoring resource • rf-domain-manager – Configures the RF Domain manager as the monitoring resource
dhcp vlan [<1-4094>| <VLAN-ALIAS-NAME>]	The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords: • 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. • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.
dns <IP/HOST-ALIAS-NAME>	The following parameters are recursive and common to the 'all', 'cluster-master', and 'rf-domain-manager' keywords: • 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. • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

{dhcp vlan {<1-4094>| <VLAN-ALIAS-NAME>]| dns <IP/HOST-ALIAS-NAME>}	The 'dhcp' and 'dns' parameters are recursive and you can optionally configure multiple VLANs and critical resource IPv4 addresses (or host alias names).
	• 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.
	  • vlan [<1-4094>|<VLAN-ALIAS-NAME>] – 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.
	• 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.
	  • <IP/HOST-ALIAS-NAME> – Configures the IPv4 address or host alias of the critical resource. Specify the IPv4 address or host alias name (should be existing and configured).

```
critical-resource monitor interval <5-86400>
```

monitor interval <5-86400>	Configures the critical resource monitoring frequency. This is the interval between two successive pings to the critical resource being monitored. • <5-86400> – Specifies the frequency in seconds. Specify the time from 5 - 86400 seconds. The default is 30 seconds.

```
critical-resource retry-count <0-10>
```

retry-count <0-10>	Configures the maximum number of failed attempts allowed to connect to a critical resource, using DHCP/DNS message flows, before marking it as down • <0-10> – Specifies the maximum number of retries from 0 - 10. The default value is 3 attempts.

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 853

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
crypto on page 930	Invokes commands used to configure ISAKMP policy, ISAKMP client, and ISAKMP peer
crypto-auto-ipsec-tunnel commands on page 936	Creates an auto IPSec VPN tunnel and enters its configuration mode
crypto-ikev1/ikev2-policy commands on page 942	Creates a crypto IKEv1/IKEv2 policy and enters its configuration mode
crypto-ikev1/ikev2-peer commands on page 947	Creates a IKEv1/IKEv2 peer and enters its configuration mode

Command	Description
crypto-map-config-commands on page 954	Creates a crypto map and enters its configuration mode
crypto-remote-vpn-client commands on page 971	Creates a remote VPN client and enters its configuration mode

crypto

crypto on page 929

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 SA *(Security Association)* 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 SPI *(Security Parameter Index)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

auto-ipsec-secure	Configures the Auto IPSec Secure parameter settings. For Auto IPSec tunnel configuration commands, see crypto-auto-ipsec-tunnel commands on page 936.
enable-ike-uniqueids	Enables IKE *(Internet Key Exchange)* unique ID check. For more information on IKE unique IDs, see remotegw on page 940.
load-management	Configures load management for platforms using software cryptography

```
crypto ike-version [ikev1-only|ikev2-only]
```

ike-version [ikev1-only|ikev2-only]	Selects and starts the IKE daemon • ikev1-only – Enables support for IKEv1 tunnels only • ikev2-only – Enables support for IKEv2 tunnels only

```
crypto ikev1 [dpd-keepalive <10-3600>|dpd-retries <1-100>|nat-keepalive <10-3600>|peer
<IKEV1-PEER>|policy <IKEV1-POLICY-NAME>|remote-vpn]
```

ikev1	Configures the IKE version 1 parameters
dpd-keepalive <10-3600>	Sets the global DPD *(Dead Peer Detection)* 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.
dpd-retries <1-1000>	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.

nat-keepalive <10-3600>	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.
peer <IKEV1-PEER>	Specify the name/Identifier for the IKEv1 peer. For IKEV1 peer configuration commands, see crypto-ikev1/ikev2-peer commands on page 947.
policy <IKEV1-POLICY-NAME>	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 crypto-ikev1/ikev2-policy commands on page 942.
remote-vpn	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]
```

ikev2	Configures the IKE version 2 parameters
cookie-challenge-threshold <1-100>	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.
dpd-keepalive <10-3600>	Sets the global DPD keepalive interval from 10 - 3600 seconds. The default is 30 seconds.
dpd-retries <1-100>	Sets the global DPD retries count from 1 - 100. The default is 5.
nat-keepalive <10-3600>	Sets the global NAT keepalive interval from 10 - 3600 seconds. The default is 20 seconds.
peer <IKEV2-PEER>	Specify the name/Identifier for the IKEv2 peer
policy <IKEV2-POLICY-NAME>	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.
remote-vpn	Specifies an IKEv2 remote-VPN server configuration (responder only)

```
crypto ipsec df-bit [clear|copy|set]
```

ipsec	Configures the IPSec policy parameters
df-bit [clear|copy|set]	Configures DF *(Don't-Fragment)* bit handling for encapsulating header. The options are: • clear – Clears the DF bit in the outer header and ignores in the inner header • copy – Copies the DF bit from the inner header to the outer header. This is the default setting. • set – Sets the DF bit in the outer header

```
crypto ipsec security-association lifetime [kilobytes <500-2147483646>|seconds
<120-86400>]
```

ipsec	Configures the IPSec policy parameters
security-association	Configures the IPSec SAs parameters

lifetime [kilobyte |seconds]	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.
	• kilobytes – Specifies a volume-based key duration (minimum is 500 KB and maximum is 2147483646 KB)
	  • <500-2147483646> – Specify a value from 500 - 2147483646 KB. The default is 4608000 KB.
	• seconds – Specifies a time-based key duration (minimum is 120 seconds and maximum is 86400 seconds)
	  • <120-86400> – Specify a value from 120 - 86400 seconds. The default is 3600 seconds.
	The security association lifetime can be overridden under crypto maps.

```
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]
```

ipsec	Configures the IPSec policy parameters
transform-set <TRANSFORM-SET-TAG>	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. • <TRANSFORM-SET-TAG> – Specify the transform set name. 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**. Note: The authentication schemes available are: esp-md5-hmac and esp-sha-hmac.
esp-3des	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.
esp-aes	Configures the ESP transform using AES *(Advanced Encryption Standard)* cipher. The transform set is assigned to a crypto map using the map's set > transform-set command.
esp-aes-192	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.
esp-aes-256	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.
esp-des	Configures the ESP transform using DES *(Data Encryption Standard)* cipher (56 bits). The transform set is assigned to a crypto map using the map's `set > transform-set` command.

esp-null	Configures the ESP transform with no encryption
[esp-aes-xcbc-mac| esp-md5-hmac| esp-sha-hmac| esp-sha256-hmac]	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: • esp-aes-xcbc-mac – Configures ESP transform using AES-XCBC authorization • esp-md5-hmac – Configures ESP transform using HMAC-MD5 authorization • esp-sha-hmac – Configures ESP transform using HMAC-SHA authorization. This is the default setting. • esp-sha256-hmac – Configures ESP transform using HMAC-SHA256 authorization

```
crypto map <CRYPTO-MAP-TAG> <1-1000> [ipsec-isakmp {dynamic}|ipsec-manual]
```

map <CRYPTO-MAP-TAG>	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. • <CRYPTO-MAP-TAG> – Specify a name for the crypto map. The name should not exceed 32 characters. For crypto map configuration commands, see crypto-map-ipsec-manual-instance on page 955.
<1-1000>	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.
ipsec-isakmp {dynamic}	Configures IPSEC w/ISAKMP. • dynamic – Optional. Configures dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration
ipsec-manual	Configures IPSEC w/manual keying. Remote configuration is not allowed for manual crypto map.

```
crypto pki import crl <TRUSTPOINT-NAME> <URL> <1-168>
```

pki	Configures certificate parameters. The PKI *(Public Key Infrastructure)* protocol creates encrypted public keys using digital certificates from certificate authorities.
import	Imports a trustpoint related configuration
crl <TRUSTPOINT-NAME>	Imports a CRL *(Certificate Revocation List)*. 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. • <TRUSTPOINT-NAME> – Specify the trustpoint name.

<URL>	Specify the CRL source address in the following format. Both IPv4 and IPv6 address formats are supported. tftp://<hostname|IPv4 or IPv6>[:port]/path/file ftp://<user>:<passwd>@<hostname|IPv4 or IPv6>[:port]/path/file sftp://<user>:<passwd>@<hostname|IPv4 or IPv6>[:port]>/path/file http://<hostname|IPv4 or IPv6>[:port]/path/file cf:/path/file usb<n>:/path/file
<1-168>	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]
```

plain-text-deny-acl-scope	Configures plain-text-deny-acl-scope parameters
global	Applies the plain text deny ACL globally. This is the default setting.
interface	Applies the plain text deny ACL to the interface only

```
crypto remote-vpn-client
```

remote-vpn-client	Configures remote VPN client settings. For more information, see crypto-remote-vpn-client commands on page 971.

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 radio1
 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

no on page 1214	Disables or reverts settings to their default

crypto-auto-ipsec-tunnel commands

crypto on page 929

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
groupid on page 937	Specifies the identity string used for IKE authentication
ip on page 938	Enables the controller or service platform to uniquely identify APs and the hosts present in the AP's subnet
ike-lifetime on page 939	Configures the IKE SA's key lifetime in seconds
ikev2 on page 940	Enables the forced re-authentication of IKEv2 peer
remotegw on page 940	Defines the IKE version used for an auto IPSec tunnel using secure gateways
no on page 941	Removes or reverts the crypto auto IPSec tunnel settings

groupid

crypto-auto-ipsec-tunnel commands on page 936

Specifies the identity string used for IKE authentication

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

<WORD>	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.
psk [0 <WORD>| 2 <WORD>| <WORD>]	Configures the PSK *(pre-shared key)* as the authentication type for secure peer authentication on the auto IPSec secure tunnel • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Specify a string value from 8 - 21 characters.
rsa	Configures the RSA *(Rivest-Shamir-Adleman)* 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 936

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip nat crypto
```

Parameters

```
ip nat crypto
```

ip nat crypto	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 remotegw on page 940 and crypto on page 930.

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 936

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ike-lifetime <600-86400>
```

Parameters

```
ike-lifetime <600-86400>
```

ike-lifetime <600-86400>	Sets the IKE SA's key lifetime in seconds • <600-86400> – Specify a value fro m 600 - 86400 seconds. The default is 8600 seconds.

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 936

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ikev2 peer reauth
```

Parameters

```
ikev2 peer reauth
```

ikev2 peer reauth	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 936

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

Parameters

```
remotegw ike-version [ikev1-aggr|ikev1-main|ikev2] {uniqueid}
```

remotegw ike-version	Configures the IKE version used for initiating auto IPSec tunnel with secure gateways other than the controller
ikev1-aggr	Aggregation mode is used by the auto IPSec tunnel initiator to set up the connection
ikev1-main	Main mode is used by the auto IPSec tunnel initiator to establish the connection

ikev2	IKEv2 is the preferred method when wireless controller/AP only is used
uniqueid	This keyword is common to all of the above parameters. • uniqueid – 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 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. After enabling unique ID assignment, enable IKE unique ID check. For more information, see crypto on page 930.

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 936

Removes or resets this auto IPSec tunnel settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [groupid|ike-lifetime|ikev2 peer reauth|ip nat crypto]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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 929

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
dpd-keepalive on page 943	Sets DPD keep alive packet interval
dpd-retries on page 944	Sets the maximum number of attempts for sending DPD keep alive packets (applicable only to the IKEv1 policy)
isakmp-proposal on page 944	Configures ISAKMP proposals
lifetime on page 945	Specifies how long an IKE SA is valid before it expires
mode on page 946	Sets the mode of the tunnels (applicable only to the IKEv1 policy)
no on page 947	Removes or reverts IKEv1/IKEv2 policy settings

dpd-keepalive

crypto-ikev1/ikev2-policy commands on page 942

Sets the DPD keep-alive packet interval

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 942

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 942

Configures ISAKMP proposals and their parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

<WORD>	Assigns the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration.
encryption [3des|aes|aes-192| aes-256]	Configures the encryption method used by the tunneled peers to securely inter-operate • 3des – Configures triple data encryption standard • aes – Configures AES (128 bit keys) • aes-192 – Configures AES (192 bit keys) • aes-256 – Configures AES (256 bit keys). This is the default setting.
group [14|2|5]	Specifies the DH *(Diffie-Hellman)* 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. • 14 – Configures DH group 14 • 2 – Configures DH group 2. This is the default setting. • 5 – Configures DH group 5
hash [maes-xcbc-mac| md5|sha| sha256]	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. • aes-xcbc-mac – Uses AES XCBC Auth hash algorithm. This option is applicable only to the IKEv2 policy configuration context. • md5 – Uses MD5 *(Message Digest 5)* hash algorithm • sha – Uses SHA *(Secure Hash Authentication)* hash algorithm. This is the default setting. • sha256 – Uses Secure Hash Standard 2 algorithm

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 942

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
lifetime <600-86400>
```

Parameters

```
lifetime <600-86400>
```

lifetime <600-86400>	Specifies how many seconds an IKE SA lasts before it expires. Set a time stamp from 600 - 86400 seconds. • <600-86400> – Specify a value from 600 - 86400 seconds. The default is 86400 seconds.

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 testpraposal encryption aes group 2 hash sha
nx9500-6C8809(config-profile-default-rfs4000-ikev1-policy-ikev1-testpolicy)#
```

mode

crypto-ikev1/ikev2-policy commands on page 942

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mode [aggresive|main]
```

Parameters

```
mode [aggresive|main]
```

mode [aggresive|main]	Sets the mode of the tunnels • aggressive – Initiates the aggressive mode • main – Initiates the main mode 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.

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 942

Removes or reverts IKEv1/IKEv2 policy settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [dpd-keepalive|dpd-retries|isakmp-proposal <WORD>|lifetime|mode]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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 929

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
authentication on page 949	Configures a peer's authentication mode and the pre-shared key
ip on page 950	Configures the peer's IP address
localid on page 950	Configures a peer's local identity details
remoteid on page 951	Configures a remote peer's identity details
use on page 952	Associates an IKEv1 policy and IKEv2 policy with the IKEv1 and IKEv2 peer respectively
no on page 953	Negates a command or reverts settings to their default. The no command, when used in the ISAKMP policy mode, defaults the ISAKMP protection suite settings.

authentication

crypto-ikev1/ikev2-peer commands on page 947

Configures IKEv1/IKEv2 peer's authentication mode and the pre-shared key

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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}
```

psk [0 <WORD>| 2 <WORD>| <WORD>] {local|remote}	Configures the authentication mode as 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. • 0 <WORD> – Configures a clear text key • 2 <WORD> – Configures an encrypted key • <WORD> – Configures the pre-shared key The following keywords are available only in the IKEv2 peer configuration mode: • local – Optional. Uses the specified key for local peer authentication only • remote – Optional. Uses the specified key for remote peer authentication only **Note:** In case the peer type is not specified, this string is used for authenticating both local and remote peers.

```
authentication rsa
```

rsa	Configures the authentication mode as 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 947

Sets the IP address or FQDN *(Fully Qualified Domain Name)* of the IPSec VPN peer used in the tunnel setup

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip [address <IP>|fqdn <WORD>]
```

Parameters

```
ip [address <IP>|fqdn <WORD>]
```

address <IP>	Specify the peer device's IP address.
fqdn <WORD>	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 947

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

address <IP>	Configures the peer's IP address. The IP address is used as local identity.
autogen-uniqueid <WORD>	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 autogen-uniqueid on page 880. • <WORD> – Provide the string.
dn <WORD>	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.
email <WORD>	Configures the peer's e-mail address. The maximum length is 128 characters.
fqdn <WORD>	Configures the peer's FQDN. The maximum length is 128 characters.
string <WORD>	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 947

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

address <IP>	Configures the remote IKEv1/IKEV2 peer's IP address. The IP address is used as the peer's remote identity.
dn <WORD>	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.
email <WORD>	Configures the remote peer's e-mail address. The maximum length is 128 characters.

fqdn <WORD>	Configures a peer's FQDN. The maximum length is 128 characters.
string <WORD>	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 947

Associates IKEv1/IKEv2 policy with the IKEv1/IKEv2 peer respectively

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use ikev1-policy <IKEV1-POLICY-NAME>
use ikev2-policy <IKEV2-POLICY-NAME>
```

Parameters

```
use ikev1-policy <IKEV1-POLICY-NAME>
```

use ikev1-policy <IKEV1-POLICY-NAME>	Specify the IKEv1 policy name. The local IKEv1 policy and the peer IKEv1 policy must have matching group settings for successful negotiations.

```
use ikev2-policy <IKEV2-POLICY-NAME>
```

use ikev2-policy <IKEV2-POLICY-NAME>	Specify the IKEv2 policy name. 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 947

Removes or reverts IKEv1/IKEv2 peer settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [authentication|ip|localid|remoteid|use <IKEv1/IKEv2-POLICY-NAME>]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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 929

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 thecrypto 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

  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-cryptomap-map1#1)#
```

The following table summarizes crypto map configuration mode commands:

Command	Description
crypto-map-ipsec-isakmp-instance on page 961	Configures an auto site-to-site VPN or remote VPN client
crypto-map-ipsec-manual-instance on page 955	Configures a manual site-to-site VPN

crypto-map-ipsec-manual-instance

crypto-map-config-commands on page 954

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:
  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

  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#3)#
```

The following table summarizes IPSec manual VPN tunnel configuration mode commands:

Command	Description
local-endpoint-ip on page 956	Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)
mode on page 957	Sets the tunnel mode
peer on page 957	Sets the peer device's IP address
security-association on page 958	Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by a crypto map
session-key on page 958	Defines encryption and authentication keys for a crypto map
use on page 960	Uses the configured IP access list
no on page 961	Removes or reverts crypto map IPSec manual settings

local-endpoint-ip

crypto-map-ipsec-manual-instance on page 955

Uses the configured IP as local tunnel endpoint address, instead of the interface IP (Advanced Configuration)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local-endpoint-ip <IP>
```

Parameters

```
local-endpoint-ip <IP>
```

local-endpoint-ip <IP>	Uses the configured IP as local tunnel's endpoint address • <IP> – Specify the IP address. The specified IP address must be available on the interface.

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 955

Sets the crypto map tunnel mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mode [transport|tunnel]
```

Parameters

```
mode [transport|tunnel]
```

mode [transport|tunnel]	Sets the mode of the tunnel for this crypto map • transport – Initiates transport mode • tunnel – Initiates tunnel mode (default setting)

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 955

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
peer <IP>
```

Parameters

```
peer <IP>
```

peer <IP>	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 955

Defines the lifetime (in kilobytes and/or seconds) of IPSec SAs created by this crypto map

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

Parameters

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

lifetime [kilobytes <500-2147483646>| seconds <120-86400>]	Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association. • kilobytes <500-2147483646> – Defines volume based key duration. Specify a value from 500 - 2147483646 bytes. • 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 955

Defines encryption and authentication keys for this crypto map

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

session-key [inbound|outbound]	Defines the manual inbound and outbound security association key parameters
ah <256-4294967295>	Configures authentication header (AH) as the security protocol for the security session • <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295 The SPI (in combination with the destination IP address and security protocol) identifies the security association.
[0|2|authenticator [md5|sha] <WORD>]	Specifies the key type • 0 – Sets a clear text key • 2 – Sets an encrypted key • authenticator – Sets AH authenticator details • md5 <WORD> – AH with MD5 authentication • sha <WORD> – AH with SHA authentication <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40

```
session-key [inbound|outbound] esp <256-4294967295> [0|2|cipher [3des|aes|aes-192|aes-256|
des|esp-null]] <WORD> authenticator [md5|sha] <WORD>
```

session-key [inbound|outbound]	Defines the manual inbound and outbound security association key parameters
esp <256-4294967295>	Configures Encapsulating Security Payloads (ESP) as the security protocol for the security session. This is the default setting. • <256-4294967295> – Sets the SPI for the security association from 256 - 4294967295 The SPI (in combination with the destination IP address and security protocol) identifies the security association.
[0|2|cipher [3des|aes|aes-192| aes-256|des| esp-null]]	• 0 – Sets a clear text key • 2 – Sets an encrypted key • cipher – Sets encryption/decryption key details • 3des – ESP with 3DES encryption • aes – ESP with AES encryption • aes-192 – ESP with AES-192 encryption • aes-256 – ESP with AES-256 encryption • des – ESP with DES encryption • esp-null – ESP with no encryption authenticator – Specify ESP authenticator details md5 <WORD> – ESP with MD5 authentication sha <WORD> – ESP with SHA authentication <WORD> – Sets security association key value. The following key lengths (in hex characters) are required (w/o leading 0x).AH-MD5: 32, AH-SHA: 40

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 955

Associates an existing IP access list with this crypto map. The ACL protects the VPN traffic.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list <IP-ACCESS-LIST-NAME>	Specify the IP access list name.

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 955

Removes or resets this crypto map's settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [local-endpoint-ip|mode|peer|security-association|session-key|use]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes or resets this crypto map settings based on the parameters passed

Example

```
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)#

nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#no use ip-access-list
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#no peer
nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#no mode

nx9500-6C8809(config-profile-default-rfs4000-cryptomap-map1#1)#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#1)#
```

crypto-map-ipsec-isakmp-instance

crypto-map-config-commands on page 954

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 this configuration mode commands:

Command	Description
ip on page 963	Enables this setting to utilize IP/Port NAT on the VPN tunnel. This command is applicable only to the site-to-site VPN tunnel.
local-endpoint-ip on page 963	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.
modeconfig on page 964	Configures the mode config method (pull or push) associated with the remote VPN client. This command is applicable only to the remote VPN client.
peer on page 964	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.
pfs on page 965	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.
remote-type on page 966	Configures the remote VPN client type as either None or XAuth. This command is applicable only to the remote VPN client.
security-association on page 967	Defines this automatic VPN tunnel's IPSec SA settings. This command is applicable to the site-to-site VPN tunnel and remote VPN client.
transform-set on page 968	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.
use on page 969	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.
no (crypto-map-ipsec-isakmp) on page 970	Removes or reverts site-to-site VPN tunnel or remote VPN client settings

ip

crypto-map-ipsec-isakmp-instance on page 961

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip nat crypto
```

Parameters

```
ip nat crypto
```

ip nat crypto	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-ipsec-isakmp-instance on page 961

Uses the configured IP as local tunnel endpoint address, instead of the interface IP

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local-endpoint-ip <IP>
```

Parameters

```
local-endpoint-ip <IP>
```

local-endpoint-ip <IP>	Configures the local VPN tunnel's (site-to-site VPN tunnel or remote VPN client) endpoint IP address • <IP> – Specify the IP address. The specified IP address must be available on the interface.

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-ipsec-isakmp-instance on page 961

Configures the mode config method (pull or push) associated with the remote VPN client

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
modeconfig [pull|push]
```

Parameters

```
modeconfig [pull|push]
```

modeconfig [pull|push]	Configures the mode config method associated with a remote VPN client. The options are: pull and push. 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-ipsec-isakmp-instance on page 961

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

Parameters

```
peer <1-3> [ikev1|ikev2] <IKEv1/IKEv2-PEER-NAME>
```

peer <1-3>	Creates a new peer and configures the peer's priority level. Peer '1' is the primary peer, and peer '3' is redundant.
ikev1 <IKEv1-PEER-NAME>	Configures an IKEv1 peer • <IKEv1-PEER-NAME> – Specify the IKEv1 peer's name.
ikev2<IKEv2-PEER-NAME>	Configures an IKEv2 peer • <IKEv2-PEER-NAME> – Specify the IKEv2 peer's name.

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-ipsec-isakmp-instance on page 961

Configures PFS *(Perfect Forward Secrecy)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
pfs [14|2|5]
```

Parameters

```
pfs [14|2|5]
```

pfs [14|2|5]	Configures PFS • 14 – Configures D-H Group14 (2048-bit modp) • 2 – Configures D-H Group2 (1024-bit modp) • 5 – Configures D-H Group5 (1536-bit modp)

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-ipsec-isakmp-instance on page 961

Configures the remote VPN client type as either None or XAuth

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
remote-type [none|xauth]
```

Parameters

```
remote-type [none|xauth]
```

remote-type [none|xauth]	Specify the remote VPN's client type • none – Configures remote VPN client with No XAUTH • xauth – Configures remote VPN client as using XAUTH (applicable only for IKEv1). This is the default setting. 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.

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-ipsec-isakmp-instance on page 961

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

inactivity-timeout <120-86400>	Specifies an inactivity period, in seconds, for this IPSec VPN SA. Once the set value is exceeded, the association is timed out. • <120-86400> – Specify a value from 120 - 86400 seconds. The default is 900 seconds.
level perhost	Specifies the granularity level for this IPSec VPN SA • perhost – Sets the IPSec VPN SA's granularity to the host level

```
security-association lifetime [kilobytes <500-2147483646>|seconds <120-86400>]
```

lifetime [kilobytes <500-2147483646>| seconds <120-86400>]	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. • kilobytes <500-2147483646> – 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. • seconds <120-86400> – 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.

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-ipsec-isakmp-instance on page 961

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

Parameters

```
transform-set <TRANSFORM-SET-TAG> {<TRANSFORM-SET-TAG>}
```

transform-set <TRANSFORM-SET-TAG> <TRANSFORM-SET-TAG>	Applies a transform set. The transform set should be existing and configured. • <TRANSFORM-SET-TAG> – Specify the transform set's name. • <TRANSFORM-SET-TAG> – Optional. Specify a second transform set. You can provide multiple, space-separated, transform set tags.

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-ipsec-isakmp-instance on page 961

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

Parameters

```
use ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list <IP-ACCESS-LIST-NAME>	Specify the 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-ipsec-isakmp)

crypto-map-ipsec-isakmp-instance on page 961

Removes or reverts the auto site-to-site VPN tunnel or remote VPN client settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [ip|local-endpoint-ip|modeconfig|peer|pfs|remote-type|security-association|transform-set|use]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes or resets this auto site-to-site/remote VPN settings based on the parameters 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-remote-vpn-client commands

crypto on page 929

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
dhcp-peer on page 973	Configures DHCP peer's local ID and authentication settings
peer on page 973	Adds a remote IKEv2 peer
shutdown on page 974	Disables the remote VPN client
transform-set on page 975	Associates an existing IPSec transform set with this remote VPN client
no on page 975	Removes the remote VPN client settings

dhcp-peer

crypto-remote-vpn-client commands on page 971

Configures DHCP peer's local ID and authentication settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

dhcp-peer authentication psk [0 <WORD>| 2 <WORD>| <WORD>]	Configures the DHCP peer's authentication type as PSK • 0 <WORD> – Configures a clear text authentication key • 2 <WORD> – Configures an encrypted authentication key • <WORD> – Provide a 8 - 21 character shared key password for DHCP peer authentication
dhcp-peer authentication rsa	Configures the DHCP peer's authentication type as RSA. This is the default setting.

```
dhcp-peer localid [autogen-uniqueid <WORD>|string <WORD>]
```

dhcp-peer localid [autogen-uniqueid <WORD>| string <WORD>]	Configures the DHCP peer's localid using one of the following options:
	• 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 autogen-uniqueid on page 880.
	  • <WORD> – Provide the string.
	• string - Uses the value provided here as the DHCP peer's localid.
	  • <WORD> - Provide the string.

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 971

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

Parameters

```
peer <1-3> ikev2 <IKEV2-PEER-NAME>
```

peer <1-3>	Adds a IKEv2 peer. You can add maximum of three (3) peers to achieve redundancy. • <1-3> – Specify a priority level for the peer from 1 - 3 (1 = primary, 2 = secondary, and 3 = redundant).
ikev2 <IKEV2-PEER-NAME>	Specify the IKEv2 peer's name. **Note:** The peer should be existing and configured. To configure an IKEv2 peer use the `crypto > ikev2 > peer > <IKEv2-PEER-NAME>` 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 971

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 971

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}
```

Parameters

```
transform-set <IPSEC-XFORM-TAG> {<IPSEC-XFORM-TAG>}
```

transform-set <IPSEC-XFORM-TAG> <IPSEC-XFORM-TAG>	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. Note: To configure a transform-set, use the `crypto > ipsec > transform-set` command in the profile or device configuration mode.

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 971

Removes the remote VPN client settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

no <PARAMETERS>	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 853

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 configures a low-disk-space threshold value.

These parameters can also be configured in the device configuration context of the NX9500, NX9600 series service platforms.

Supported in the following platforms:

- Service Platforms — NX9500, 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>
```

database backup database [captive-portal| nsight]	Backs up captive portal and/or NSight database to a specified location and file. Select the database to backup.
	• database – Selects the database to backup
	  • captive-portal – Backs up captive portal database
	  • nsight – Backs up NSight database
	After specifying the database type, configure the destination location and file name.

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

```
database low-disk-space-threshold <10-50>
```

database low-disk-space-threshold <10-50>	Configures the low disk space threshold for syslog warning. Once the threshold value configured here is reached a syslog warning is sent. • <10-50> – Specify the threshold from 10 - 50. The default is 30.

Example

```
nx9500-6C8809(config-profile-testNX9500)#database backup database nsight ftp://
anonymous:anonymous@192.168.13.10/backups/nsight/nsight.tar.gz
```

Related Commands

no on page 1214	Removes database backup configurations

device-onboard

Profile Config Commands on page 853

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 1548.

Supported in the following platforms:

- Service Platforms — NX9500, NX9600, VX9000

Syntax

```
device-onboard [logo|title] <WORD>
```

Parameters

```
device-onboard [logo|title] <WORD>
```

device-onboard [logo|title] <WORD>	Configures the logo and page title displayed on the device-onboarding portal • logo – Specify the logo image file name. Note, logo image dimensions must not exceed 109 pixel and 52 pixel in width and height respectively. • title – Specify the UI portal title. Note, the title should not exceed 32 characters in length. The following keyword is common to both of the above parameters: • <WORD> – Specify the logo image file name/page title.

```
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

no on page 1214	Removes the device-onboarding UI portal's logo image file name and title configuration

device-upgrade

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
device-upgrade [add-auto|auto|count|persist-images]
device-upgrade add-auto [(ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000)]
device-upgrade auto {(ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000)}
device-upgrade count <1-128>
device-upgrade persist-images
```

Parameters

```
device-upgrade add-auto[(ap505|ap510|rfs4000||nx5500|nx75xx| nx9000|nx9600)]
```

device-upgrade add-auto	Configures a list of devices 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.
[<DEVICE-TYPE>]	Specifies the type of devices to be upgraded. Select the device type. The options are: The options are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000. **Note:** Multiple device types can be added to the add-auto list.

```
device-upgrade auto {(ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|nx9600|vx9000)}
```

device-upgrade auto	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.
<DEVICE-TYPE>	Optional. Specifies the type of device to be lined up for automatic firmware upgrade. The options are: The options are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000. **Note:** Multiple device types can be added to the auto list.

```
device-upgrade count <1-128>
```

device-upgrade count <1-128>	Configures the maximum number of concurrent upgrades possible • <1-128> – specify a value from 1 - 128. The default is 10.

```
device-upgrade persist-images
```

device-upgrade	Configures parameters for automatic firmware upgrade of adopted devices. Use this command to select the device types and the maximum number of concurrent upgrades.
persist-images	Enables RF Domain manager to retain AP firmware image after upgrade, subject to availability of space. This option is enabled by default. 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 ap71xx

rfs4000-229D58config-profile-default-rfs4000)#show context
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 device-upgrade auto ap71xx
 device-upgrade persist-ap-image
 crypto ikev1 policy ikev1-default
  qos trust 802.1p
--More--
rfs4000-229D58(config-profile-default-rfs4000)#
```

Related Commands

no on page 1214	Removes device firmware upgrade settings on this profile
device-upgrade on page 706 (show commands)	Displays device upgrade details

diag

Profile Config Commands on page 853

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 623.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
diag pkts
```

Parameters

```
diag pkts
```

diag pkts	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

no on page 1214	Disables looped packet logging

dot1x

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Dot1x supplicant capabilities is supported on the following platforms:

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
```

system-auth-control	Enables system auth control. Enables dot1x authorization globally for the controller. This feature is disabled by default.

```
dot1X holdtime <0-600>
```

holdtime <0-600>	Configures a holdtime value. This is the interval after which an authentication attempt is ignored or failed. • <0-600> – Specify a value from 0 - 600 seconds. A value of '0' indicates no holdtime. The default is 600 seconds or 10 minutes. 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
```

guest-vlan	Configures guest VLAN and supplicant behavior. This feature is disabled by default.
supplicant	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>
```

use aaa-policy <AAA-POLICY-NAME>	Associates a specified 802.1x AAA policy (for MAC authentication) with this access point profile • <AAA-POLICY-NAME> – Specify the AAA policy name. Once specified, this AAA policy is utilized for authenticating user requests.

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

no on page 1214	Disables or reverts settings to their default

dpi

Profile Config Commands on page 853

Enables DPI *(Deep Packet Inspection)* 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 — AP505, AP510
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}
```

dpi	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.
custom-app <CUSTOM-APP-NAME>	Optional. Adds custom application to this profile • <CUSTOM-APP-NAME> – Specify custom application name (should be existing and configured) If no custom application is specified, the system detects the PACE built-in applications. Note: For more information on application categories and application detection, see application on page 183.

```
dpi {logging [level [<0-7>|alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]|on]}
```

dpi	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.
logging [level [<0-7>| alerts|critical| debugging| emergencies|errors| informational| notifications| warnings]|on]	Optional. Enables DPI logging and sets the logging level • level – Configures the DPI logging level. Use one of the following options to specify the logging level: • <0-7> Logging severity level • alerts Immediate action needed (1) • critical Critical conditions (2) • debugging Debugging messages (7) • emergencies System is unusable (0) • errors Conditions (3) • nformational Informational messages (6) • notifications Normal but significant conditions (5) - Default setting • warnings Warning conditions (4) Either specify the logging level index (from 0 - 7) or the description. For example, to log all alerts either enter '1' or 'alerts'. • on – Enables application detection event logging. DPI logging is disabled by default.

```
dpi {metadata [http|ssl|voice-video]}
```

dpi	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.
metadata [http|ssl|voice-video]	Optional. Enables metadata extraction from following flows: • http – HTTP flows. This option is disabled by default. • ssl – SSL flows. This option is disabled by default. • voice-video – Voice and video classified flows. This option is disabled by default.

```
dpi {metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}}
```

dpi	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.
metadata tcp-rtt {app-group <APPLICATION-GROUP-NAME>}	Optional. Enables TCP-RTT *(Transmission Control Protocol - Round Trip Time)* metadata collection for application groups. Before executing this command, ensure that you have created at least one application group. 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. • app-group – Optional. Specifies the customized application-group name containing the applications for which TCP-RTT is to be collected • <APPLICATION-GROUP-NAME> – 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. For more information on creating customized application-groups, see application-group on page 191 . 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.

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

no on page 1214	Disables DPI (application assurance) on this profile

dscp-mapping

Profile Config Commands on page 853

Configures IP DSCP *(Differentiated Services Code Point)* to 802.1p priority mapping for untagged frames

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dscp-mapping <WORD> priority <0-7>
```

Parameters

```
dscp-mapping <word> priority <0-7>
```

<WORD>	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.
priority <0-7>	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: • 0 – Best effort • 1 – Background • 2 – Spare • 3 – Excellent effort • 4 – Controlled load • 5 – Video • 6 – Voice • 7 – Network control **Note:** 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.

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 me1
 interface ge1
```

```
 ip dhcp trust
 qos trust dscp
nx9500-6C8809(config-profile-default-rfs4000)#
```

Related Commands

no on page 1214	Disables or reverts settings to their default

eguest-server (VX9000 only)

Profile Config Commands on page 853

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 1280.

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 267.

Syntax

```
eguest-server
```

Parameters

```
eguest-server
```

eguest-server	**Note:** Execute this command, without the 'host' option, on the EGuest server. When executed, the EGuest daemon is enabled on the host. EGuest server can be hosted only a VX 9000 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

no on page 1214	Disables the EGuest server by stopping the EGuest daemon

eguest-server (NOC Only)

Profile Config Commands on page 853

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 1280.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}
```

Parameters

```
eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}
```

eguest-server <1-3> host <IPv4/IPv6/HOSTNAME> {http|https}	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. • <1-3> – Configures the EGuest server index number. A maximum of three EGuest servers can be configured. • host <IPv4/IPv6/HOSTNAME> – Configures the EGuest server's IPv4/IPv6 address or hostname. {http|https} – Optional. Configures the mode of connection as HTTP or HTTPS. **Note:** HTTPS is recommended as it uses encryption for transmission and is therefore more secure.

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

no on page 1214	Removes the EGuest server IP address/hostname configuration

email-notification

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

recipient <RECIPIENT-EMAIL>	Defines the recipient's e-mail address. A maximum of 6 (six) e-mail addresses can the configured. • <RECIPIENT-EMAIL> – Specify the recipient's e-mail address (should not exceed 64 characters in length).

```
email-notification host <SMTP-SERVER-IP/HOSTNAME> sender <SENDER-EMAIL> [(port <1-65535>,
security [none|ssl|starttls], username <SMTP-USERNAME> password [2 <WORD>|<WORD>])]
```

host <SMTP-SERVER-IP/ HOSTNAME>	Configures the host SMTP server's IP address or hostname • <SMTP-SERVER-IP/HOSTNAME> – Specify the SMTP server's IP address or hostname.
sender <SENDER-EMAIL>	Defines the sender's e-mail address. This is the from address on notification e-mails. • <SENDER-EMAIL> – Specify the sender's e-mail address (should not exceed 64 characters in length). Use the email-notification > recipient > <EMAIL-ADDRESS> command to configure the recipient's address.

port <1-65535>	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. • <1-65535> – Specify the port from 1 - 65535.
security [none|ssl|starttls]	This option is recursive and applicable to the 'port' and 'username' parameters. Configures the SMTP encryption type used • none – No encryption used • ssl – Uses SSL *(Secure Sockets Layer)* encryption between the SMTP server and the client • starttls – Uses STARTTLS encryption between the SMTP server and the client
username <SMTP-USERNAME> password [2 <WORD>| <WORD>]	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. • <SMTP-USERNAME> – Specify the SMTP username (should not exceed 64 characters in length). • password – Configures the SMTP server password. Specify the password associated with the username of the sender on the outgoing SMTP server. 2 <WORD> – Configures an encrypted password <WORD> – Specify the password (should not exceed 127 characters in length).

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

no on page 1214	Disables or reverts settings to their default

enforce-version

Profile Config Commands on page 853

Enables checking of a device's firmware version before attempting adoption or clustering

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

Parameters

```
enforce-version [adoption|cluster] [full|major|minor|none|strict]
```

adoption	Verifies firmware versions before adopting. This option is enabled by default.
cluster	Verifies firmware versions before clustering. This option is enabled by default.
full	Allows adoption or clustering when the first four octets of the firmware versions match (for example 5.9.3.0)
major	Allows adoption or clustering when the first two octets of the firmware versions match (for example 5.9)
minor	Allows adoption or clustering when the first three octets of the firmware versions match (for example 5.9.3)
none	Allows adoption or clustering between any firmware versions
strict	Allows adoption or clustering only when firmware versions exactly match (for example 5.9.3.0-010D). 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 pppoe1
 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

no on page 1214	Disables or reverts settings to their default

environmental-sensor

Profile Config Commands on page 853

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]
```

environmental-sensor	Configures environmental sensor settings on this profile
humidity	Enables (turns on) humidity sensors. This setting is enabled by default.
motion	Enables (turns on) motion sensors.This setting is enabled by default.
polling-interval <1-100>	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. • <1-100> – Specify a value from 1 - 100 seconds. The default is 5 seconds.
temperature	Enables (turns on) temperature sensors. This setting is enabled by default.

```
environmental-sensor light {holdtime <10-201>|radio-shutdown [all|radio-1| radio-2]}
```

environmental-sensor	Configures environmental sensor settings on this profile
light	Enables (turns on) light sensors and specifies its settings 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.

holdtime <10-201>	Optional. Configures a holdtime, in seconds, for the light sensor • <10-201> – Specify a value from 10 - 201 seconds. The default value is 11 seconds.
radio-shutdown [all|radio1|radio2]	Optional. Shuts down the sensor's radios • all – Shuts down all radios. This is the default setting. • radio1 – Shuts down radio 1 • radio2 – Shuts down radio 2 AP8132's using this profile have their radios shut down, when the radio's power falls below the specified threshold. Use the `environmental-sensor > light > threshold > [high|low]` command to set the threshold values.

```
environmental-sensor light {threshold [high <100-10000>|low <0-1000>]}
```

environmental-sensor	Configures environmental sensor settings on this profile
light	Enables (turns on) light sensors and specifies its settings
threshold	Optional. Configures the upper and lower thresholds for the amount of light in the environment
high <100-10000>	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. The light sensor triggers an event if the amount of light exceeds the specified value.
low <0-1000>	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. 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

no on page 1214	Removes the environmental sensor's settings

events

Profile Config Commands on page 853

Displays system event messages

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
events [forward on|on]
```

Parameters

```
events [forward on|on]
```

forward on	Forwards system event messages to the wireless controller, service platform, or cluster members. This feature is enabled by default. • on – Enables forwarding of system events
on	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

no on page 1214	Disables or reverts settings to their default

export

Profile Config Commands on page 853

Enables export of startup.log file after every boot

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

export startup-log	Enables export of the startup.log file after every boot. This option is disabled by default.
max-retries <2-65535>	Configures the maximum number of retries in case the export process fails • <2-65535> – Specify a value from 2 - 65535.
retry-interval <30-86400>	Configures the interval between two consecutive retries • <30-86400> – Specify a value from 30 - 86400 seconds.
url <URL>	Configures the destination URL in the following format: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file 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

no on page 1214	Disables export of startup.log file

file-sync

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
file-sync [auto|count <1-20>]
```

Parameters

```
file-sync [auto|count <1-20>]
```

file-sync [auto|count <1-20>]	Configures the following file-synching parameters: • 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. 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: `file-sync > load-file > <URL>`. • count <1-20> – Configures the maximum number of access points that can be concurrently auto-installed. • <1-20> – Specify a value from 1 - 20. The default is 10 access points. **Note:** For the NX 95XX and NX 96XXservice platforms the count-range is from 1 - 128.

```
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

no on page 1214	Disables automatic file syncing between the staging-controller and its access points

floor

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
floor <WORD> {<1-4094>}
```

Parameters

```
floor <WORD> {<1-4094>}
```

floor <WORD> {<1-4094>}	Sets the floor name where the target device is located • <WORD> – Specify the floor name (should not exceed 64 characters in length). • <1-4094> – Optional. Configures the floor number from 1 - 4094. The default is 1.

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

no on page 1214	Resets the configured floor name and number

gre

Profile Config Commands on page 853

The following table summarizes commands that allow you to enter the GRE configuration mode:

Command	Description
gre on page 998	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.
gre-config-instance on page 1000	Summarizes GRE tunnel configuration mode commands

gre

gre on page 997

Enables GRE *(Generic Routing Encapsulation)* 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>
```

gre tunnel <GRE-TUNNEL-NAME>	Creates a new GRE tunnel or modifies an existing GRE tunnel • <GRE-TUNNEL-NAME> – If creating a new tunnel, specify a unique name for it. If modifying an existing tunnel, specify its name.

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

no on page 1214	Disables GRE tunneling on this profile

gre-config-instance

gre on page 997

The following table summarizes GRE tunnel configuration mode commands:

Command	Description
dscp on page 1000	Sets the GRE tunnel's DSCP / 802.1q priority value
establishment-criteria on page 1001	Configures the GRE tunnel establishment criteria
failover on page 1002	Enables periodic pinging of the primary gateway to assess its availability, in case it is unreachable
mtu on page 1002	Configures the MTU for IPv4/IPv6 L2GRE tunnel endpoints
native on page 1003	Configures native trunking settings for this GRE tunnel
no on page 1004	Removes the GRE tunnel settings based on the parameters passed
peer on page 1005	Configures the GRE tunnel's end-point peers
tunneled-vlan on page 1006	Defines the VLAN that connected clients use to route GRE-tunneled traffic within their respective WLANs

dscp

gre-config-instance on page 1000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dscp [<0-63>|reflect]
```

Parameters

```
dscp [<0-63>|reflect]
```

dscp <0-63>	Specifies the DSCP 802.1q priority value for outer packets from 0 - 63. The default is 1.
dscp reflect	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

no on page 1004	Removes the GRE tunnel settings based on the parameters passed

establishment-criteria

gre-config-instance on page 1000

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 — AP505i, AP510i/e, AP560i/h
- 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>]
```

establishment-criteria [always| cluster-master| rf-domain-manager| vrrp-master <1-255>]	Configures the GRE tunnel establishment criteria. The options are: • 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. • cluster-master – Establishes tunnel only if the tunnel device is designated as the cluster master • rf-domain-manager – Establishes tunnel only if the tunnel device is designated as the RF Domain manager • vrrp-master <1-255> – Establishes tunnel only if the tunnel device is designated as the Virtual Router Redundancy (VRRP) master • <1-255> – 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.

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 1000

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 — AP505i, AP510i/e, AP560i/h
- 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>
```

failover interval <1-250> retry <1-10>	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. • <1-250> – Specify a value from 1 - 250 seconds. • retry – Specifies the maximum number attempts made to ping the primary gateway before the session is terminated. <1-10> – Specify a value from 1 - 10.

Example

```
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#failover
interval 200 retry 5

rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#show context
 gre tunnel testGRETunnel
  dscp 20
  failover interval 200 retry 5
rfs4000-229D58(config-device 00-23-68-22-9D-58-gre-tunnel-testGRETunnel)#
```

Related Commands

no on page 1004	Removes the GRE tunnel settings based on the parameters passed

mtu

gre-config-instance on page 1000

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 — AP505i, AP510i/e, AP560i/h
- 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>]
```

mtu [ipv4 <900-1476>| ipv6 <1236-1456>]	Configures the MTU for L2GRE tunnel endpoints • ipv4 <900-1476> – Configures IPv4 L2GRE tunnel endpoint MTU from 900 - 1476. The default is 1476. • ipv6 <1236-1456> – Configures IPv6 L2GRE tunnel endpoint MTU from 1236 - 1456. The default is 1456.

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 1000

Configures native trunking settings for this GRE tunnel

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
native [tagged|vlan <1-4094>]
```

Parameters

```
native [tagged|vlan <1-4094>]
```

native tagged	Enables native VLAN tagging 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. 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.
native vlan <1-4094>	Specifies a numerical VLAN ID (1 - 4094) for the native VLAN 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.

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

no on page 1004	Removes the GRE tunnel settings based on the parameters passed

no

gre-config-instance on page 1000

Removes or resets the GRE tunnel settings based on the parameters passed

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- 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>
```

no <PARAMETERS>	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 1000

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 — AP505i, AP510i/e, AP560i/h
- 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>
```

peer <1-2> ip <IPv4/IPv6>	Configures the tunnel's end-point peers • <1-2> – Specify a numeric index for each peer to help differentiate the tunnel end points. • ip – Specify the IP address (IPv4/IPv6) of the added GRE peer to serve as a network address identifier. <IPv4/IPv6> – Specify the peer's IPv4 or IPv6 address.

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

no on page 1004	Removes the GRE tunnel settings based on the parameters passed

tunneled-vlan

gre-config-instance on page 1000

Defines the VLAN that connected clients use to route GRE tunneled traffic within their respective WLANs

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
tunneled-vlan <VLAN-ID>
```

Parameters

```
tunneled-vlan <VLAN-ID>
```

tunneled-vlan <VLAN-ID>	Specifies the VLANs associated with this GRE tunnel • <VLAN-ID> – Specify the VLAN IDs. Specify a comma-separated list of IDs, to specify multiple VLANs. For example, 1,10,12,16-20.

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-testGRETunnel)#
```

Related Commands

no on page 1004	Removes the GRE tunnel settings based on the parameters passed

http-analyze

Profile Config Commands on page 853

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 NOC *(Network Operations Center)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

http-analyze	Configures HTTP analysis related parameters
compress	Compresses update files before forwarding to the controller. This option is disabled by default.
update-interval <1-3600>	Configures the interval, in seconds, at which buffered packets are pushed to the controller • <1-3600> – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.

```
http-analyze external-server [password <WORD>|proxy <URL>|update-interval| url|username|
validate-server-certificate]
```

http-analyze external-server	Configures the external HTTP analytics engine's parameters
password <WORD>	Configures the external analytics engine's password • <WORD> – Provide the login password. This is the password associated with the user name needed to access the external analytics engine.
proxy <URL>	Configures the proxy server's URL • <URL> – Specify the proxy server's URL in the following format: http://username:password@proxy-server:port. For example, http://mot:sym@wwwgate0.mot.com:1080
update-interval <1-36000>	Configures the interval, in seconds, at which buffered packets are pushed to the external analytics engine • <1-3600> – Specify the interval from 1 - 3600 seconds. The default is 60 seconds.
url <URI>	Configures the external analytics engine's IP address or URL • <URL> – Provide the IP address or URL.
username <WORD>	Configures the user name needed to access the external analytics engine • <WORD> – Provide the user name.
validate-server-certificate	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

no on page 1214	Disables HTTP analyze settings

interface

Profile Config Commands on page 853

The following table summarizes interface configuration commands:

Command	Description
interface on page 1010	Selects an interface to configure
interface-config-ge-instance on page 1013	Summarizes Ethernet interface (associated with the wireless controller or service platform) configuration commands
interface-config-vlan-instance on page 1044	Summarizes VLAN interface configuration commands
interface-config-port-channel-instance on page 1058	Summarizes port-channel interface configuration commands
interface-config-radio-instance on page 1072	Summarizes radio interface configuration commands (applicable to devices with built-in radios)
interface-config-wwan-instance on page 1144	Summarizes WWAN interface configuration commands
interface-config-bluetooth-instance on page 1152	Summarizes the Bluetooth radio interface configuration commands

interface

interface on page 1009

Selects an interface to configure

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to device type. 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>|t1e1 <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>|t1e1 <1-4>|up <1-2>|vlan <1-4094>|wwan1|xge <1-4>]
```

<INTERFACE-NAME>	Enters the configuration mode of the interface identified by the <INTERFACE-NAME> keyword
bluetooth <1-1>	Selects the Bluetooth radio interface • <1-1> – Specify the Bluetooth radio interface index from 1 - 1. As of now only one Bluetooth radio interface is supported. This interface is applicable only for the AP8432 and AP8533 model access points.
fe <1-4>	Selects a FastEthernet interface • <1-4> – Specify the interface index from 1 - 4.
ge <1-24>	Selects a GigabitEthernet interface • <1-24> – Specify the interface index from 1 - 24. .
me1	Selects a management interface
port-channel <1-4>	Selects the port channel interface • <1-4> – Specify the interface index from 1 - 4.
pppoe1	Selects the PPP over Ethernet interface to configure
radio [1|2|3]	Selects a radio interface • 1 – Selects radio interface 1 • 2 – Selects radio interface 2 • 3 – Selects radio interface 3 The radio interface is not available on wireless controllers or service platforms.
up1	Selects the uplink GigabitEthernet interface
vlan <1-4094>	Selects a VLAN interface • <1-4094> – Specify the SVI VLAN ID from 1 - 4094.
wwan1	Selects a Wireless WAN interface This interface is applicable only to AP7161, AP8163, RFS4000 model access points and controllers.
xge <1-4>	Selects a TenGigabitEthernet interface • <1-2> – Specify the interface index from 1 - 4.

Usage Guidelines

GE ports are available on WiNG controllers and access points, such as the NX9500 service paltform and AP510. GE ports are RJ-45 supporting 10/100/1000Mbps.

The ports available on a device vary depending on the model type. For example, the following ports are available on NX series service platforms:

- NX7500 - ge1-ge10, xge1-xge2
- NX9500 series - ge1, ge2, xge1-xge4

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.

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.

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.

The following ports are available on the new super-spec access points:

- AP510 - GE1/POE (LAN), GE2/POE (LAN)
- AP505 - GE1/POE (LAN), GE2 (LAN)

Example

To access an AP's interface configuration mode, in the AP's profile or device context, issue the following commands:

```
ap505-13403B(config-device-94-9B-2C-13-40-38)#interface ?
  WORD          Interface name
  bluetooth     Bluetooth interface
  fe            Select a FastEthernet interface
  ge            Select a GigabitEthernet interface
  me1           Select the management interface
  port-channel  Select a port channel interface
  radio         Select a radio
  up1           Select the Uplink GigabitEthernet interface
  vlan          Select a vlan interface (switched virtual interface)
  xge           Select a TenGigabitEthernet interface

ap505-13403B(config-device-94-9B-2C-13-40-38)#interface

ap505-13403B(config-device-94-9B-2C-13-40-38-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 opreation 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

ap505-13403B(config-device-94-9B-2C-13-40-38-if-bluetooth1)#

nx9500-6C8809(config-profile-test510)#interface radio 1
nx9500-6C8809(config-profile-test510-if-radio1)#?
Radio Mode commands:
  adaptivity                Adaptivity
  aeroscout                 Aeroscout 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
--More--
nx9500-6C8809(config-profile-test510-if-radio1)#
```

Related Commands

no on page 1214	Removes the selected interface

interface-config-ge-instance

interface on page 1009

This section documents the GigabitEthernet configuration commands.

The following ports are available to NX series service platform models:

- NX 5500: ge1, ge2
- NX 7500: ge1-ge10, xge1-xge2
- NX 9000 series - ge1, ge2 (10GigE ports (xge1-xge4) are available on NX9610 models)

The *GE* ports are RJ-45 ports supporting 10/100/1000 Mbps or 10/100/1000/2500/5000 Mbps.

The *UP* ports supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone because it has a non-blocking 1gbps connection unlike the GE ports.

The following ports are available on access points:

- AP505i: GE1/POE (LAN), GE2 (LAN)
- AP510i/e: GE1/POE (LAN), GE2/POE (LAN)
- AP560i/h: GE1/POE (LAN), GE2/POE (LAN)

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
captive-portal-enforcement on page 1015	Enables captive-portal enforcement on this Ethernet port
cdp on page 1016	Enables CDP *(Cisco Discovery Protocol)* on this Ethernet port
channel-group on page 1016	Assigns this Ethernet port to a channel group
description on page 1017	Configures a description for this Ethernet port
dot1x (authenticator) on page 1018	Configures 802.1X authenticator settings
dot1x (supplicant) on page 1021	Configures 802.1X supplicant settings
duplex on page 1022	Specifies the duplex mode for the interface
eee on page 1023	Enables EEE *(Energy-Efficient Ethernet)* mode on the selected GE port.
ip on page 1024	Sets the IP address for this Ethernet port
ipv6 on page 1025	Sets the DHCPv6 and ICMPv6 ND *(neighbor discovery)* components for this interface
lacp on page 1027	Configures the selected GE port's LACP *(Link Aggregation Control Protocol)* port-priority value
lacp-channel-group on page 1028	Configures the selected GE port as a member of a port-channel group (also referred as LAG)
lldp on page 1029	Configures LLDP *(Link Local Discovery Protocol)*
mac-auth on page 1030	Enables MAC-based authentication on this Ethernet port

Command	Description
no on page 1031	Removes or reverts the selected Ethernet port settings
power on page 1032	Configures PoE *(Power over Ethernet)* settings on this interface
qos on page 1033	Enables QoS
shutdown on page 1034	Disables the selected Ethernet port
spanning-tree on page 1034	Configures spanning tree parameters
speed on page 1036	Specifies the speed on this Ethernet port
switchport on page 1037	Sets interface switching mode characteristics
use on page 1042	Associates IPv4, IPv6, and/or MAC ACL with the selected Ethernet port

captive-portal-enforcement

interface-config-ge-instance on page 1013

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:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
captive-portal-enforcement {fall-back}
```

Parameters

```
captive-portal-enforcement {fall-back}
```

captive-portal-enforcement fall-back	Enables captive-portal enforcement on this Ethernet port • 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.

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

no on page 1031	Disables captive-portal enforcement on this interface

cdp

interface-config-ge-instance on page 1013

Enables CDP on the selected GE port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cdp [receive|transmit]
```

Parameters

```
cdp [receive|transmit]
```

receive	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.
transmit	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

no on page 1031	Disables CDP packet snooping on the controller or service platform's selected GE ports

channel-group

interface-config-ge-instance on page 1013

Assigns this Ethernet port to a channel group. Ethernet ports can be aggregated to form a channel group. They 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
channel-group <1-4>
```

Parameters

```
channel-group <1-4>
```

<1-4>	Specifies a channel group number from 1 - 4. The number of channel groups supported varies with the device type. For example: • NX5500 – Supports three channel groups • NX75XX – Supports four channel groups • NX95XX – Supports two channel groups **Note:** RFS4000 – Supports three channel groups.

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 1031	Removes the channel group to which this port belongs

description

interface-config-ge-instance on page 1013

Configures a description for this Ethernet port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
description [<LINE>|<WORD>]
```

Parameters

```
description [<LINE>|<WORD>]
```

<LINE>	Configures the maximum length (number of characters) of the interface description
<WORD>	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 1031	Removes the interface description

dot1x (authenticator)

interface-config-ge-instance on page 1013

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 —AP505i, AP510i/e, AP560i/h
- Wireless Controllers — 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]]
```

dot1x authenticator	Configures 802.1x authenticator settings
guest-vlan <1-4094>	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.

host-mode [multi-host| single-host]	Configures the host mode for this interface • multi-host – Configures multiple host mode • single-host – Configures single host mode. This is the default setting.
max-reauth-req <1-10>	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. • <1-10> – Specify a value from 1 -10. The default is 2.
port-control [auto| force-authorized| force-unauthorized]	Configures port control state • auto – Configures auto port state • force-authorized – Configures authorized port state. This is the default setting. • force-unauthorized – Configures unauthorized port state
reauthenticate	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.
timeout [quiet-period|reauth-period] <1-65535>	Configures timeout settings for this interface • quiet-period – Configures the quiet period timeout in seconds. This is the interval, in seconds, between successive client authentication attempts. • reauth-period – Configures the time after which re-authentication is initiated The following option is common to 'quiet-period' and 'reauth-period' keywords: • <1-65535> – Specify a 'quiet-period' or 'reauth-period' from 1 - 65535 seconds.

Example

```
nx9500-6C8809(config-profile-testNX5500-if-ge1)#dot1x authenticator guest-vlan 2

nx9500-6C8809(config-profile-testNX5500-if-ge1)#dot1x authenticator host-mode multi-host

nx9500-6C8809(config-profile-testNX5500-if-ge1))#dot1x authenticator max-reauth-req 6

nx9500-6C8809(config-profile-testNX5500-if-ge1)#dot1x authenticator reauthenticate

nx9500-6C8809(config-profile-testNX5500-if-ge1)#show context
 interface ge1
  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
nx9500-6C8809(config-profile-testNX5500-if-ge1)#
```

The following examples show the configurations made on an NX5500 to enable it as a dot1X authenticator:

1 Configure AAA policy on the authenticator, and identify the authentication server as onboard (self):

```
NX5500-229D58(config-aaa-policy-aaa-wireddot1x)#show context
aaa-policy aaa-wireddot1x
```

```
authentication server 1 onboard controller
NX5500-229D58(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:

```
nx5500-229D58(config-radius-user-pool-wired-dot1x-users)#show con
radius-user-pool-policy wired-dot1x-users
user bob password 0 bob1234
nx5500-229D58(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 1021 section.

3 Configure RADIUS server policy on the authenticator, and associate the RADIUS user policy created in the previous step:

```
nx5500-229D58(config-radius-server-policy-for-wired-dot1x)#show con
radius-server-policy for-wired-dot1x
use radius-user-pool-policy wired-dot1x-users
nx5500-229D58(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:

```
nx5500-229D58(config-device-00-15-29-22-9D-58)#use radius-server-policy for-wired-dot1x
```

5 In the authenticator's interface > ge configuration mode, configure the following parameters:

```
nx5500-229D58(config-device-00-15-29-22-9D-58-if-ge2)#dot1x authenticator host-mode
single-host
nx5500-229D58(config-device-00-15-29-22-9D-58-if-ge2)#dot1x authenticator port-control
auto
```

6 In the authenticator's self configuration mode, configure the following parameters:

```
nx5500-229D58(config-device-00-15-29-22-9D-58)#dot1x system-auth-control
nx5500-229D58(config-device-00-15-29-22-9D-58)#dot1x use aaa-policy aaa-wireddot1x
```

Following example displays the above configured parameters:

```
nx5500-229D58(config-device-00-15-29-22-9D-58)#show context
use profile default-nx5500
use rf-domain default
hostname nx5500-229D58
 use radius-server-policy for-wired-dot1x
interface me1
  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--
nx5500-229D58(config-device-00-15-29-22-9D-58)
```

Related Commands

no on page 1031	Disables or reverts interface settings to their default

dot1x (supplicant)

interface-config-ge-instance on page 1013

Enables IEEE 802.1X port-based authentication on the selected wired port and configures the credentials required to authenticate the iEEE 802.1X-capable supplicant (client).

The IEEE 802.1X port-based authentication protocol restricts unauthorized LAN access by enforcing supplicant authentication at the port. When a supplicant associates with a IEEE 802.1X enabled wired port, normal traffic across the port is suspended until the supplicant is successfully authenticated. Once the supplicant is successfully authenticated, the port status changes to authorized and normal traffic flow resumes. During the suspended state, only EAP over LAN traffic is allowed across the wired port.

The 802.1X port-based authentication process consists of the following three components:

- supplicant - the client (wired-device) that is attempting to access the network
- authenticating server - the server (e.g., RADIUS server) used to authenticate the client..
- authenticator - the access point or switch that proxies the client's request to the authenticating server

The authentication methods supported are username/password and EAP-TLS (trustpoint-based authentication).

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Wireless Controllers — NX5500, NX7500

Syntax

```
dot1x supplicant [username|trustpoint]
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
dot1x supplicant trustpoint <WORD>
```

Parameters

```
dot1x supplicant username <USERNAME> password [0 <WORD>|2 <WORD>|<WORD>]
```

dot1x supplicant	Configures 802.1x suppliant settings
username <USERNAME>	Sets the username for authentication • <USERNAME> – Specify the supplicant's username.
password [0 <WORD>| 2 <WORD>| <WORD>]	Sets the password associated with the supplicant's username. Select any one of the following options: • 0 <WORD> – Sets a clear text password • 2 <WORD> – Sets an encrypted password • <WORD> – Specify the password.

```
dot1x supplicant trustpoint <WORD>
```

dot1x supplicant	Configures 802.1x suppliant settings
trustpoint <WORD>	Sets the authentication mode as EAP-TLS and specifies the trustpoint to be used for authentication. In EAP-TLS authentication, the supplicant and RADIUS server authenticate each other using certificates. 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. • <WORD> – Specify the trustpoint name.

Example

```
nx9500-6C8809(config-profile-testAP505-if-ge2)#dot1x supplicant username test
password 0 test123

nx9500-6C8809(config-profile-testAP505-if-ge2)#show context
 interface ge2
  dot1x supplicant username test password 0 test123
nx9500-6C8809(config-profile-testAP505-if-ge2)#
```

The following configuration enables dot1X supplicant on AP510 profile:

```
nx9500-6C8809(config-profile-testAP510-if-ge2)#dot1x supplicant trustpoint test

nx9500-6C8809(config-profile-testAP510-if-ge2)#show context
 interface ge2
  dot1x supplicant trustpoint test
nx9500-6C8809(config-profile-testAP510-if-ge2)#
```

Related Commands

no on page 1031	Removes 802.1X supplicant (client) settings

duplex

interface-config-ge-instance on page 1013

Configures duplex mode (for the flow of packets) on this Ethernet port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
duplex [auto|half|full]
```

Parameters

```
duplex [auto|half|full]
```

auto	Enables automatic duplexity on an interface port. The port automatically detects whether it should run in full or half-duplex mode. (default setting)
half	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.
full	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

no on page 1031	Reverts to default (auto)

eee

Enables *Energy-Efficient Ethernet* (EEE) on the selected GE port. The IEEE 802.3az standard, also known as EEE, defines a set of enhancements that allows physical layer transmitters to consume less power when they are in a state of idleness or low data activity. By enabling EEE, you allow the network port to switch between an **`active mode`** (during data transmission) and **`idle mode`** (when there is no Ethernet traffic).

IEEE 802.3az refers to this state of idleness as *Low Power Idle* (LPI). When enabled, in the LPI mode, both ends of the Ethernet link disable operating circuitry that are not needed and save power.

Note

Energy-Efficient Ethernet can be activated only if devices at both ends of the physical link support EEE.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i

Syntax

```
eee
```

Parameters

```
none
```

Example

```
ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#eee
```

The following command shows the state of Energy-efficient Ethernet, where:

- **Enable**: Indicates if Energy-Efficient Ethernet is *enabled* or *disabled* on the selected physical port. A value of '1' indicates enabled and '0' indicates disabled.
- **Active**: Indictaes if Energy-Efficient Ethernet is *active* or *inactive* on the selected physical port. A value of '1' indicates EEE is active and '0' indicates inactive. Note, will be active only if the devices on both ends of the phhysical link support EEE.

```
ap505-13403B#show interface ge 1
Interface ge2 is UP
  Hardware-type: ethernet, Mode: Layer 2, Address: 94-9B-2C-13-40-39
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 1G, Maximum 2.5G
  Duplex: Admin Auto, Operational Full
  EEE: Enable 1, Active 1
  Active-medium: n/a
  Switchport settings: access, access-vlan: 1
    Input packets 0, bytes 0, dropped 0
    Received 0 unicasts, 0 broadcasts, 0 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 0, bytes 0, dropped 0
    Sent 0 unicasts, 0 broadcasts, 0 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions

ap505-13403B#
```

Related Commands

no on page 1031	Disables EEE on the selected GE port

ip

interface-config-ge-instance on page 1013

Sets the ARP and DHCP components for this Ethernet port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip [arp|dhcp]
ip [arp [header-mismatch-validation|trust]|dhcp trust]
```

Parameters

```
ip [arp [header-mismatch-validation|trust]|dhcp trust]
```

arp [header-mismatch-validation| trust]	Configures ARP packet settings • 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. • 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.
dhcp trust	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.

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

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
  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

no on page 1031	Removes the ARP and DHCP components configured for this interface

ipv6

interface-config-ge-instance on page 1013

Sets the DHCPv6 and ICMPv6 ND *(neighbor discovery)* 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 NS *(neighbor solicitation)* and NA *(neighbor advertisement)* 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 ink 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|nd]
ipv6 dhcpv6 trust
ipv6 nd [header-mismatch-validation|raguard|trust]
```

Parameters

```
ipv6 dhcpv6 trust
```

ipv6 dhcpv6 trust	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. A DHCPv6 server can be connected to a DHCPv6 trusted port.

```
ipv6 nd [header-mismatch-validation|raguard|trust]
```

ipv6 nd	Configures IPv6 ND settings
header-mismatch-validation	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.
raguard	Allows redirection of RAs *(router advertisements)* 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.
trust	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-ge1)#ipv6 dhcpv6 trust

nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd header-mismatch-validation
nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge1)#ipv6 nd trust

nx9500-6C8809(config-device-B4-C7-99-6D-CD-4B-if-ge1)#show context
interface ge1
  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-ge1)#
```

Related Commands

no on page 1031	Removes or reverts IPv6 settings on this interface

lacp

interface-config-ge-instance on page 1013

Configures the selected GE port's LACP *(Link Aggregation Control Protocol)* port-priority value. If LACP is enabled, and the selected port is a member of a LAG *(link aggregation group)*, 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 1028 command to configure this port as a LAG member.

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, 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 1031	Removes the selected GE port's configured port-priority value

lacp-channel-group

interface-config-ge-instance on page 1013

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, NX9500, NX9600, VX9000

Syntax

```
lacp-channel-group <1-4> mode [active|passive]
```

Parameters

```
lacp-channel-group <1-4> mode [active|passive]
```

lacp-channel-group <1-4>	Associates this GE port with an existing port-channel group • <1-4> – Specify a value from 1 - 4. Use the `interface > port-channel > <1-4>` command to configure a port-channel group. For more information, see interface-config-port-channel-instance on page 1058.
mode [active|passive]	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. • 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. • passive – Configures the port as passive member. When set to passive, the port will only respond to LACPDU received from its corresponding Active port. 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 lacp on page 1279.

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

no on page 1031	Removes the selected GE port's port-channel group membership

lldp

interface-config-ge-instance on page 1013

Configures LLDP *(Link Local Discovery Protocol)* parameters on this Ethernet port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
lldp [receive|transmit]
```

Parameters

```
lldp [receive|transmit]
```

receive	Enables LLDP PDUs *(Protocol Data Units)* snooping. When enabled, the port receives periodic updates from a multicast address informing about presence of neighbors. This option is enabled by default.
transmit	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

no on page 1031	Disables or reverts interface settings to their default

mac-auth

interface-config-ge-instance on page 1013

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 1197.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 1031	Disables authentication of MAC addresses on the selected wired port

no

interface-config-ge-instance on page 1013

Removes or reverts the selected Ethernet port settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [captive-portal-enforcement|cdp|channel-group|description|dot1x|duplex|eee|
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 eee
no ip [arp [header-mismatch-validation|trust]|dhcp trust]
no ipv6 [dhcpv6 trust|nd [header-mismatch-validation|raguard|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>
```

no <PARAMETERS>	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
ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#show context
 interface ge2
  eee
ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#n

ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#no eee

ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#show context
 interface ge2
  no eee
ap505-13403B(config-device-94-9B-2C-13-40-38-if-ge2)#
```

power

interface-config-ge-instance on page 1013

Configures PoE *(Power over Ethernet)* settings on the selected physical interface. Allows you to monitor port power consumption and configure power usage limits and priorities for each GE port.

Note

The following ports are available on the new super-spec access points:

- AP510 - GE1/POE (LAN), GE2/POE (LAN)
- AP505 - GE1/POE (LAN), GE2 (LAN)

Supported in the following platforms:

- Access Points — AP505, AP510
- 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]}
```

power	Configures power related thresholds for this interface
best-effort	Optional. Enables power when the device is not operating from an 802.3at class 4 power source. Note: POE power best effort configuration not available on AP505 and AP510 model access points.
limit <0-40>	Optional. Configures the PoE power limit from 0 - 40 Watts. The default is 30 Watts.
priority [critical|high|low]	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/access point. • critical – Sets PoE priority as critical • high – Sets PoE priority as high • low – Sets PoE priority as low. This is the default setting.

Example

```
nx9500-6C8809(config-profile-testAP505-if-ge1)#power limit 30

nx9500-6C8809(config-profile-testAP505-if-ge1)#power priority critical

nx9500-6C8809(config-profile-testAP505-if-ge1)#show context
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
  power limit 30
  power priority critical
nx9500-6C8809(config-profile-testAP505-if-ge1)#
```

Related Commands

no on page 1031	Removes PoE settings on this interface

qos

interface-config-ge-instance on page 1013

Defines QoS *(Quality of Service)* settings on this Ethernet port

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
qos trust [802.1p|cos|dscp]
```

Parameters

```
qos trust [802.1p|cos|dscp]
```

trust [802.1p|cos|dscp]	Trusts QoS values ingressing on this interface • 802.1p – Trusts 802.1p COS values ingressing on this interface • cos – Trusts 802.1p COS values ingressing on this interface. This option is enabled by default. • dscp – Trusts IP DSCP QOS values ingressing on this interface. This option is enabled by default.

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#qos trust dscp

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#qos trust 802.1p

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
  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

no on page 1031	Removes QoS settings on the selected interface

shutdown

interface-config-ge-instance on page 1013

Shuts down (disables) an interface. The interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
shutdown
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#shutdown
```

Related Commands

no on page 1031	Disables or reverts interface settings to their default

spanning-tree

interface-config-ge-instance on page 1013

Configures spanning tree parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|
port-cisco-interoperability|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]
```

force-version <0-3>	Specifies the spanning tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select one of the following versions: • 0 – Spanning Tree Protocol (STP) • 1 – Not supported • 2 – Rapid Spanning tree Protocol (RSTP) • 3 – Multiple Spanning Tree Protocol (MSTP). This is the default setting
guard root	Enables Root Guard for the port The Root Guard disables superior BPDU *(Bridge Protocol Data Unit)* 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.
portfast	Enables rapid transitions. Enabling PortFast allows the port to bypass the listening and learning states.

```
spanning-tree [bpdufilter|bpduguard] [default|disable|enable]
```

bpdufilter [default|disable| enable]	Sets a PortFast BPDU filter for the port Use the no parameter with this command to revert the port BPDU filter to its default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.
bpduguard [default|disable| enable]	Enables BPDU guard on a port Use the no parameter with this command to set BPDU guard to its default. 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]
```

link-type [point-to-point|shared]	Enables point-to-point or shared link types • 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. • 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,

```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
```

mst <0-15>	Configures MST on a spanning tree
cost <1-200000000>	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.
port-priority <0-240>	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]
```

port-cisco-interoperability	Enables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP)
enable	Enables CISCO Interoperability
disable	Disables CISCO Interoperability. The default is disabled.

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#spanning-tree bpdufilter 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 bpdufilter 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

no on page 1031	Removes spanning tree settings configured on this interface

speed

interface-config-ge-instance on page 1013

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
speed [10|100|1000|auto]
```

Parameters

```
speed [10|100|1000|auto]
```

10	Forces 10 Mbps operation
100	Forces 100 Mbps operation
1000	Forces 1000 Mbps operation
auto	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

no on page 1031	Resets speed to default (auto)

switchport

interface-config-ge-instance on page 1013

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
swithcport 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>]
```

access vlan [<1-4094>| <VLAN-ALIAS-NAME>]	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. • <1-4094> – Specify the SVI VLAN ID from 1 - 4094. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name (should be existing and configured). 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.

```
switchport mode [access|trunk]
```

mode [access|trunk]	Sets the interface's switching mode to access or trunk (can only be used on physical - layer 2 - interfaces) • 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. • 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.

```
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

trunk allowed	Sets trunking mode, allowed VLANs characteristics of the port. Use this option to add VLANs that exclusively send packets over the listed port.

vlan [<VLAN-ID>| add <VLAN-ID>| none| remove <VLAN-ID>	Sets allowed VLAN options. The options are:
	• <VLAN-ID> – 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.)
	• none – Allows no VLANs to transmit or receive through the layer 2 interface
	• add <VLAN-ID> – Adds VLANs to the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	• remove <VLAN-ID> – Removes VLANs from the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	Allowed VLANs are configured only when the switching mode is set to “trunk”.

```
switchport trunk fabric-attach vlan [<1-4094>|<VLAN-ALIAS-NAME>] isid <1-16777214>
```

trunk	Sets trunking mode characteristics of this Ethernet port
fabric-attach	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. The Fabric Attach topology type allows an AP to attach to a SPB *(Shortest Path Bridging)* (Fabric Connect) Network. The client component on the AP communicates directly with the server on an edge switch (or it can communicate with the server through a proxy) to allow the AP to request VLAN to I-SID (backbone Service Identifier [IEEE 802.1 ah] mappings). 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. Note: When Fabric Attach is configured, LLDP (Link Layer Discovery Protocol) is automatically enabled on all APs associated with the topology. The setting cannot be disabled by users. The switch requires that the VLAN/I-SID mapping is unique per port per switch, therefore only one AP per switch port is allowed. WiNG devices connected to an FA-enabled edge switch auto-learn interface configuration from the edge switch. The WiNG device auto-configures the VLAN on that interface supplied from the edge switch. The edge switch may mark/unmark the VLAN for tagging and this reflects in the interface configuration of the WiNG device. The auto-configuration is local to the AP/controller and does not persist across reboots. It is recommended that you enable “no auto-learn staging-config” on the controller adopting the AP. We also recommend that the controller has the AP’s interface configuration pre-configured on the AP's profile, to avoid the controller overriding the AP’s configuration, resulting in the AP losing connectivity with the controller. Use this command to configure the I-SID *(Individual Service Identifier)* to VLAN mapping that the FA Client uses to negotiate with the FAS. Note: You can configure FA Client capability on a device’s profile as well as device contexts. Note: This option is enabled only when the switching mode is set to trunk.

vlan [<1-4094>|<VLAN-ALIAS-NAME>]	Configures the VLAN through which traffic from this device is routed to the FA switch • <1-4094> – Specify the VLAN from 1 - 4094. • <VLAN-ALIAS-NAME> – Use a VLAN alias to specify the VLAN. If using a VLAN alias, ensure that the alias is existing and configured. 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. Note: 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.
isid <1-16777214>	Configures the I-SID to be associated with the VLAN interface specified above. • isid <1-16777214> – 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. Note: A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port.

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

trunk	Sets trunking mode characteristics of the switchport

native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]	Configures the native VLAN ID for the trunk-mode 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. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
	• 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.
	• vlan [<1-4094>|<VLAN-ALIAS-NAME>] – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode.
	  • <1-4094> – Specify a value from 1 - 4094.
	  • <VLAN-ALIAS-NAME> – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.

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

no on page 1031	Disables or reverts interface settings to their default

use

interface-config-ge-instance on page 1013

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

ip-access-list in <IPv4-ACCESS-LIST-NAME>	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. • in – Applies the IPv4 ACL on incoming packets • <IPv4-ACCESS-LIST-NAME> – Specify the IPv4 access list name (it should be an existing and configured).
ipv6-access-list in <IPv6-ACCESS-LIST-NAME>	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. • in – Applies the IPv6 ACL on incoming packets • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name (it should be an existing and configured).
mac-access-list in <MAC-ACCESS-LIST-NAME>	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. • in – Applies the MAC ACL on incoming packets • <MAC-ACCESS-LIST-NAME> – Specify the MAC access list name (it should be an existing and configured).

Example

```
nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#use mac-access-list in test

nx9500-6C8809(config-profile-default-rfs4000-if-ge1)#use ip-access-list in test

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 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-ge1)#
```

Related Commands

no on page 1031	Disassociates the IP access list or MAC access list from the interface

interface-config-vlan-instance

interface on page 1009

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
crypto on page 1045	Defines the encryption module used with this VLAN interface
description on page 1045	Defines the VLAN interface description
dhcp on page 1046	Enables inclusion of optional fields (client identifier) in DHCP client requests
dhcp-relay-incoming on page 1047	Allows an onboard DHCP server to respond to relayed DHCP packets on this interface
ip on page 1047	Configures the VLAN interface's IP settings

Commands	Description
ipv6 on page 1050	Configures the VLAN interface's IPv6 settings
no on page 1055	Removes or reverts this VLAN interface's settings to default
shutdown on page 1056	Shuts down this VLAN interface
use on page 1057	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 1044

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 954.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

```
crypto map <CRYPTO-MAP-NAME>
```

map <CRYPTO-MAP-NAME>	Attaches a crypto map to the selected VLAN interface. The crypto map should be existing and configured. • <CRYPTO-MAP-NAME> – Specify the crypto map name.

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

no on page 1055	Disables or reverts interface VLAN settings to their default

description

interface-config-vlan-instance on page 1044

Defines this VLAN interface's description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax
`description <WORD>`

Parameters

```
description <WORD>
```

description <WORD>	Configures a description for this VLAN interface (should not exceed 64 characters in length) • <WORD> – Specify a description unique to the VLAN's specific configuration, to help differentiate it from other VLANs with similar configurations.

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

no on page 1055	Removes the VLAN interface description

dhcp

interface-config-vlan-instance on page 1044

Enables inclusion of optional fields (client identifier) in DHCP client requests. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax
`dhcp client include client-identifier`

Parameters

```
dhcp client include client-identifier
```

dhcp client include client-identifier	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

no on page 1055	Disables inclusion of client identifier in DHCP client requests

dhcp-relay-incoming

interface-config-vlan-instance on page 1044

Allows an onboard DHCP server to respond to relayed DHCP packets. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 1055	Disables or reverts interface VLAN settings to their default

ip

interface-config-vlan-instance on page 1044

Configures the VLAN interface's IP settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

helper-address <IP>	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. • <IP> – Specify the IP address of the DHCP or BOOTP server.

```
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}
```

address	Sets the VLAN interface's IP address
<IP/M>	Specifies the interface IP address in the A.B.C.D/M format • secondary – Optional. Sets the specified IP address as a secondary address
<NETWORK-ALIAS-NAME>	Uses a pre-defined network alias to provide this VLAN interface's IP address. Specify the network alias name. • secondary – Optional. Sets the network-alias provided IP address as the secondary address
zeroconf {secondary}	Uses Zero Configuration Networking (zeroconf) to generate an IP address for this interface.
	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. • secondary – Optional. Sets the generated IP address as a secondary address

```
ip address dhcp
```

address	Sets the VLAN interface's IP address
dhcp	Uses a DHCP client to obtain an IP address for this VLAN interface

```
ip dhcp client request options all
```

dhcp	Uses a DHCP client to configure a request on this VLAN interface
client	Configures a DHCP client

request	Configures DHCP client request
options	Configures DHCP client request options
all	Configures all DHCP client request options

```
ip nat [inside|outside]
```

nat [inside|outside]	Defines NAT settings for the VLAN interface. NAT is disabled by default. • 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. • 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.

```
ip ospf authentication [message-digest|null|simple-password]
```

ospf authentication	Configures OSPF authentication scheme. Options are message-digest, null, and simple-password.
message-digest	Configures md5 based authentication
null	No authentication required
simple-password	Configures simple password based authentication

```
ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]
```

ospf authentication-key	Configures an OSPF authentication key
simple-password [0 <WORD>|2 <WORD>]	Configures a simple password OSPF authentication key • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

```
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
```

bandwidth <1-10000000>	Configures bandwidth for the physical port mapped to this layer 3 interface • <1-10000000> – Specify the bandwidth from 1 - 10000000.
cost <1-65535>	Configures OSPF cost • <1-65535> – Specify OSPF cost value from 1 - 65535.
priority <0-255>	Configures OSPF priority • <0-255> – Specify OSPF priority value from 0 - 255.

```
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

ospf message-digest	Configures message digest authentication parameters
key-id <1-255>	Configures message digest authentication key ID from 0 - 255
md5 [0 <WORD>|2 <WORD>]	Configures md5 key • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

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

no on page 1055	Removes or resets IP settings on this interface

ipv6

interface-config-vlan-instance on page 1044

Configures the VLAN interface's IPv6 settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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-PORTION/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)}
```

ipv6 accept ra	Enables processing of router advertisements (RAs) on this VLAN interface. This option is enabled by default. 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.
no-default-router	Optional. Disables inclusion of routers on this interface in the default router selection process. This option is disabled by default.
no-hop-limit	Optional. Disables the use of RA advertised hop-count value on this interface. This option is disabled by default.
no-mtu	Optional. Disables the use of RA advertised MTU value on this interface. This option is disabled by default.

```
ipv6 address [<IPv6/M>|autoconfig]
```

ipv6 address [<IPv6/M>|autoconfig]	Configures IPv6 address related settings on this VLAN interface • <IPv6> – Specify the non-link local static IPv6 address and prefix length of the interface in the X:X::X:X/M format. • 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 > ipv6 > address > autoconfig command to negate the use of prefixes received in RAs.

```
ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]
```

ipv6 address eui-64	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. 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. In the EUI-64 IPv6 address the prefix and host portions are each 64 bits in length.
<IPv6/M>	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. Any bits of the configured value exceeding the prefix-length "M" are ignored and replaced by the host portion derived from the MAC address. For example: Prefix portion provided using this command: `ipv6 > address > eui-64 > 2004:b055:15:dead::1111/64`. Host portion derived using the interface's MAC address (00-15-70-37-FB-5E): 215:70ff:fe37:fb5e Auto-configured IPv6 address using the above prefix and host portions: 2004:b055:15:dead:215:70ff:fe37:fb5e/64 In this example, the host part "::1111" is ignored and replaced with the modified eui-64 formatted host address.
prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>	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. • <WORD> – 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. • <IPv6-PREFIX/PREFIX-LENGTH> – Specify the IPv6 address subnet and host parts along with prefix length (site-renumbering). For example: Prefix portion provided using this command: ipv6 > address > eui-64 > prefix-from-provider > ISP1-prefix > 2002::/64 Host portion derived using the interface's MAC address (00-15-70-37-FB-5E): 215:70ff:fe37:fb5e Auto-configured IPv6 address using the above prefix and host portions: 2002::215:70ff:fe37:fb5e/64

```
ipv6 address prefix-from-provider <WORD> <HOST-PORTION/LENGTH>]
```

ipv6 address	Configures the IPv6 address related settings on this VLAN interface
prefix-from-provider <WORD> <HOST-PORTION/LENGTH>	Configures the “prefix-from-provider” named object and the host portion of the IPv6 interface address. The prefix derived from the specified “prefix-from-provide” and the host portion (second parameter) are combined together (using the prefix-length of the specified “prefix-from-provide”) to generate the interface’s IPv6 address. • <WORD> – Provide the “prefix-from-provider” object’s name. This is the IPv6 general prefix (32 character maximum) name provided by the service provider. • <HOST-PORTION/LENGTH> – 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 <WORD> keyword.

```
ipv6 address link-local <LINK-LOCAL-ADD>
```

ipv6 address	Configures the IPv6 address related settings on this VLAN interface
link-local <LINK-LOCAL-ADD>	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 `no > ipv6 > link-local` command to restore the default link-local address derived from MAC address. It is mandatory for an IPv6 interface to always have a link-local address.

```
ipv6 dhcp [client [information|prefix-from-provider <WORD>]|relay destination <DEST-IPv6-ADD>]
```

ipv6 dhcp client [information| prefix-from-provider <WORD>]	Configures DHCPv6 client-related settings on this VLAN interface • 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. • 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.
relay destination <DEST-IPv6-ADD>	Enables DHCPv6 packet forwarding on this VLAN interface • destination – Forwards DHCPv6 packets to a specified DHCPv6 relay • <DEST-IPv6-ADD> – Specify the destination DHCPv6 relay’s address. 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.

```
ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcp-options]
```

ipv6	Configures IPv6 settings on this VLAN interface
enable	Enables IPv6 on this interface. This option is disabled by default.
enforce-dad	Enforces Duplicate Address Detection (DAD) on wired ports. This option is enabled by default.
mtu <1280-1500>	Configures the Maximum Transmission Unit (MTU) for IPv6 packets on this interface • <1280-1500> – Specify a value from 1280 - 1500. The default is 1500.

redirects	Enables ICMPv6 redirect messages sending on this interface. This option is enabled by default.
request-dhcp-options	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}
```

ipv6 router-advertisements	Configures IPv6 RA related settings on this VLAN interface
prefix <IPv6-PREFIX>	Configures a static prefix and its related parameters. The configured value is advertised on RAs. • <IPv6-PREFIX> – Specify the IPv6 prefix.
prefix-from-provider <WORD>	Configures a static "prefix-from-provider" named object and its related parameters on this VLAN interface. The configured value is advertised on RAs. • <WORD> – Specify the "prefix-from-provider" named object's name
no-autoconfig	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • 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.
off-link	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • 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.
site-prefix <SITE-PREFIX>	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • site-prefix <SITE-PREFIX> – Configures subnet (site) prefix
valid-lifetime [<30-4294967294>| at| infinite] (preferred-lifetime)	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • valid-lifetime – Configures the valid lifetime for the prefix • preferred-lifetime – Configures preferred lifetime for the prefix • <30-4294967294> – Configures the valid/preferred lifetime in seconds • at – Configures expiry time and date of the valid/preferred lifetime infinite – Configures the valid/preferred lifetime as infinite

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

no on page 1055	Removes or resets IPv6 settings on this VLAN interface

no

interface-config-vlan-instance on page 1044

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

no <PARAMETERS>	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 1044

Shuts down the selected interface. Use the no shutdown command to enable an interface.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 1055	Disables or reverts interface VLAN settings to their default

use

interface-config-vlan-instance on page 1044

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

bonjour-gw-discovery-policy <POLICY-NAME>	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. • <POLICY-NAME> – Specify the Bonjour GW Discovery policy name (should be existing and configured).
ip-access-list in <IP-ACCESS-LIST-NAME>	Uses a specified IPv4 access list with this interface • in – Applies IPv4 ACL to incoming packets • <IP-ACCESS-LIST-NAME> – Specify the IPv4 access list name.
ipv6-access-list in <IPv6-ACCESS-LIST-NAME>	Uses a specified IPv6 access list with this interface • in – Applies IPv6 ACL to incoming packets • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name.
ipv6-router-advertisement-policy <POLICY-NAME>	Uses an existing IPv6 router advertisement policy with this VLAN interface. • <POLICY-NAME> – Specify the IPv6 router advertisement policy name (should be existing and configured).
url-filter <URL-FILTER-NAME>	Enforces URL filtering on this VLAN interface by associating a URL filter • <URL-FILTER-NAME> – Specify the URL filter name (should be existing and configured).

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

no on page 1055	Disables or reverts interface VLAN settings to their default

interface-config-port-channel-instance

interface on page 1009

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-channel1)# 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-channel1)#
```

Commands	Description
description on page 1059	Configures a brief description for this port-channel interface
duplex on page 1059	Configures the duplex-mode (that is the data transmission mode) for this port-channel interface
ip on page 1060	Configures ARP and DHCP related security parameters on this port-channel interface
ipv6 on page 1061	Configures IPv6 related parameters on this port-channel interface
no on page 1063	Removes or reverts to default this port-channel interface's settings
shutdown on page 1065	Shutsdown this port-channel interface
spanning-tree on page 1065	Configures spanning-tree related parameters on this port channel interface
speed on page 1067	Configures the speed at which this port-channel interface receives and transmits data

Commands	Description
switchport on page 1068	Configures the packet switching parameters for this port-channel interface
use on page 1070	Configures access controls on this port-channel interface

description

interface-config-port-channel-instance on page 1058

Configures a brief description for this port channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
description <LINE>
```

Parameters

```
description <LINE>
```

description <LINE>	Configures a description for this port-channel interface that uniquely identifies it from other port channel interfaces • <LINE> – Provide a description not exceeding 64 characters in length.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#description "This port
-channel is for enabling dynamic LACP."

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no on page 1063	Removes this port-channel interface's description

duplex

interface-config-port-channel-instance on page 1058

Configures the duplex-mode (that is the data transmission mode) for this port channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
duplex [auto|half|full]
```

Parameters

```
duplex [auto|half|full]
```

duplex [auto|half|full]	Configures the mode of data transmission as auto, full, or half • 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. • full – Select this option to simultaneously transmit data to and from the port channel. • 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.

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

no on page 1063	Reverts the duplex-mode to the default value (auto)

ip

interface-config-port-channel-instance on page 1058

Configures ARP and DHCP related security parameters on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip [arp|dhcp]

ip arp [header-mismatch-validation|trust]

ip dhcp trust
```

Parameters

```
ip arp [header-mismatch-validation|trust]
```

ip arp [header-mismatch-validation| trust]	Configures ARP related parameters on this port-channel interface • header-mismatch-validation – Enables a source MAC mismatch check in both the ARP and ethernet headers. This option is enabled by default. • 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.

```
ip dhcp trust
```

ip dhcp trust	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

no on page 1063	Removes or reverts to default the ARP and DHCP security parameters configured

ipv6

interface-config-port-channel-instance on page 1058

Configures IPv6 related parameters on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|nd]

ipv6 dhcpv6 trust

ipv6 nd [header-mismatch-validation|raguard|trust]
```

Parameters

```
ipv6 dhcpv6 trust
```

ipv6 dhcpv6 trust	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]
```

ipv6 nd [header-mismatch-validation| raguard|trust]	Configures IPv6 neighbor discovery (ND) parameters • 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.
raguard	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.
trust	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

no on page 1063	Removes or reverts to default the IPv6 related parameters on this port-channel interface

port-channel

interface-config-port-channel-instance on page 1058

Configures client load balancing parameters on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

Parameters

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

port-channel load-balance [src-dst-ip| src-dst-mac]	Specifies whether port channel load balancing is conducted using a source/destination IP or a source/destination MAC. • src-dst-ip – Uses a source/destination IP to conduct client load balancing. This is the default setting. • src-dst-mac – Uses a source/destination MAC to conduct client load balancing

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

no on page 1063	Removes or reverts to default the client load balancing parameters on this port-channel interface

qos

interface-config-port-channel-instance on page 1058

Configures Quality of Service (QoS) related parameters on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
qos trust [802.1p|dscp]
```

Parameters

```
qos trust [802.1p|dscp]
```

qos trust [802.1p|dscp]	Configures the following QoS related parameters: • 802.1p – Trusts 802.1p class of service (COS) values ingressing on this port channel. This option is enabled by default. • dscp – Trusts IP DSCP QOS values ingressing on this port channel. This option is enabled by default.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#qos trust dscp
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
```

Related Commands

no on page 1063	Removes the QoS related parameters configured on this port-channel interface

no

interface-config-port-channel-instance on page 1058

Removes or reverts to default this port-channel interface's settings

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no beacon [description|duplex|ip|ipv6|port-channel|qos|shutdown|
spanning-tree| speed|switchport|use]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes or reverts to default this port-channels interface's settings based on the parameters passed • <PARAMETERS> – Specify the parameters.

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-channel1)#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-channel1)#

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no duplex
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no ip arp trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no ipv6 nd trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#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-channel1)#show context
 interface port-channel1
  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 1058

Shutsdown this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

shutdown

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#shutdown
```

Related Commands

no on page 1063	Re-enables this port-channel interface

spanning-tree

interface-config-port-channel-instance on page 1058

Configures spanning-tree related parameters on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|
port-cisco-interoperability|portfast]

spanning-tree [bpdufilter|bpduguard] [default|disable|enable]

spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-
interoperability [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]
```

spanning-tree [bpdufilter| bpduguard]	Configures the following BPDU related parameters for this port channel:
	• bpdufilter – Configures the BPDU filtering options. The options are:
	  • default – When selected, makes the bridge BPDU filter value to take effect. This is the default setting.
	  • disable – Disables BPDU filtering
	  • enable – Enables BPDU filtering. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs.
	• bpduguard – Configures the BPDU guard options. The options are
	  • default – When selected, makes the bridge BPDU guard value to take effect. This is the default setting.
	  • disable – Disables guarding this port from receiving BPDUs
	  • enable – Enables BPDU guarding. Enabling the BPDU guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed.
	Execute the portfast command to ensure that fast transitions is enabled on this port channel before configuring BPDU filtering and guarding.

```
spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-interoperability
[disable|enable]]
```

spanning-tree [force-version <0-3>| guard root| portfast| port-cisco-interoperability [disable|enable]	Configures the following MSTP related parameters for this port channel: • force-version <0-3> – Sets the protocol version to either STP(0), Not Supported(1), RSTP(2) or MSTP(3). MSTP is the default setting • guard root – 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. 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. • portfast – 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. • port-cisco-interoperability [disable|enable] – Enables or disables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This option is disabled by default.

```
spanning-tree link-type [point-to-point|shared]
```

spanning-tree link-type [point-to-point| shared]	Configures the link type applicable on this port channel. The options are: • 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. • 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.

```
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
```

spanning-tree mst <0-15> [cost <1-200000000>| port-priority <0-240>]	Configures the following MST parameters on this port: • mst <0-15> – Select the MST instance from 0 - 15. • cost <1-200000000> – 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. • port-priority <0-240> – Configures the port priority from 0 - 240. The lower the priority, greater is the likelihood of the port becoming a designated port.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree portfast
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree bpdufilter 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 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

no on page 1063	Removes or reverts to default the spanning-tree related parameters configured on this port channel interface

speed

interface-config-port-channel-instance on page 1058

Configures the speed at which this port-channel interface receives and transmits data

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, 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

no on page 1063	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 1058

Configures the VLAN switching parameters for this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

access vlan [<1-4094>| <VLAN-ALIAS-NAME>]	Configures the VLAN to which this port-channel interface is mapped when the switching mode is set to access. • <1-4094> – Specify the SVI VLAN ID from 1 - 4094. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name (should be existing and configured).

```
switchport mode [access|trunk]
```

mode [access|trunk]	Configures the VLAN switching mode over the port channel • access – If selected, the port channel accepts packets only form 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. • 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.

```
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
```

trunk allowed	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.

vlan [<VLAN-ID>| add <VLAN-ID>| none| remove <VLAN-ID>	Use this keyword to add/remove the allowed VLANs
	• <VLAN-ID> – 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.)
	• none – Allows no VLANs to transmit or receive through the layer 2 interface
	• add <VLAN-ID> – Adds VLANs to the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	• remove <VLAN-ID> – Removes VLANs from the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	Allowed VLANs are configured only when the switching mode is set to “trunk”.

```
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

trunk	If configuring the VLAN switching mode as trunk, use this option to configure the native VLAN on this port channel.

native [tagged| vlan [<1-4094>|<VLAN-ALIAS-NAME>]]	Configures the native VLAN ID for the trunk-mode 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. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
	• 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.
	• vlan [<1-4094>|<VLAN-ALIAS-NAME>] – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode.
	  • <1-4094> – Specify a value from 1 - 4094.
	  • <VLAN-ALIAS-NAME> – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.

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

no on page 1063	Removes the packet switching parameters configured on this port-channel interface

use

interface-config-port-channel-instance on page 1058

Configures access controls on this port-channel interface

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

use [ip-access-list| ipv6-access-list| mac-access-list] <IP/IPv6/MAC-ACCESS-LIST-NAME>]	Associates an access list controlling the inbound traffic on this port channel. • 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. • 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. • mac-access-list – Specify the MAC specific firewall rules to apply to this profile's port channel configuration. • <IP/IPv6/MAC-ACCESS-LIST-NAME> – Provide the IPv4, IPv6, or MAC access list name based on the option selected. The access list specified should be existing and configured.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#use ip-access-list in
BROADCAST-MULTICAST-CONTROL

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
  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-channel1)#
```

Related Commands

no on page 1063	Removes the access controls configured on this port-channel interface

interface-config-radio-instance

interface on page 1009

This section documents radio interface configuration parameters applicable only to the access point profiles and devices.

The new AP5XX access points are dual radio access point models.

AP505i radio and antenna specifications:

- Number of Radios: 2
  - Radio 1: Band locked at 2.4GHz. provides *Bluetooth Low Energy* (BLE) support
  - Radio 2: Band locked at 5 GHz
- Number of Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

AP510i radio and antenna specifications:

- Number of Radios: 2
  - Radio 1: Dual-band, supporting 2.4GHz and 5 GHz, provides BLE support
  - Radio 2: Band locked at 5 GHz
- Number of Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

AP510e radio and antenna specifications:

- Number of Radios: 2
  - Radio 1: Dual-band, supporting 2.4GHz and 5 GHz, provides BLE support
  - Radio 2: Band locked at 5 GHz
- Number of Antennas:
  - Eight WiFi external antennas, with the antenna ports grouped into:
    group 1 - 1, 2, 3, and 4
    group 2 - 5, 6, 7 and 8
  - One BLE internal antenna

AP560i radio and antenna specifications:

- Number of Radios: 2
  - Radio 1: Dual-band, supporting 2.4GHz and 5 GHz, provides BLE support
  - Radio 2: Band locked at 5 GHz
- Number of Antennas:
  - Eight WiFi internal antennas
  - One BLE internal antenna

AP560h radio and antenna specifications:

- Number of Radios: 2
  - Radio 1: Dual-band, supporting 2.4GHz and 5 GHz, provides BLE support
  - Radio 2: Band locked at 5 GHz

- Number of Antennas:
  - Eight WiFi internal antennas, supporting the following internal antenna modes:
    30 degree
    70 degree
  - One BLE internal antenna

To enter the AP's **profile → radio** interface context, issue the following commands:

```
<DEVICE>(config)#profile <AP-TYPE> <PROFILE-NAME>

nx9500-6C8809(config)#profile ap505 test505
nx9500-6C8809(config-profile-test505)#

nx9500-6C8809(config-profile-test505)#interface radio 2
nx9500-6C8809(config-profile-test505-if-radio2)#

nx9500-6C8809(config-profile-test505-if-radio2)#?
Radio Mode commands:
  adaptivity                  Adaptivity
  aeroscout                   Aeroscout 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-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
  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
  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
  rf-mode                      Configure the rf-mode of operation for this
                               radio
  rifs                         Configure Reduced Interframe Spacing (RIFS)
                               parameters
  rts-threshold                Configure the RTS threshold
  rx-sensitivity-reduction     Configure radio receive sensitivity reduction
                               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-test505-if-radio2)#
```

The following table summarizes the radio interface configuration commands:

Commands	Description
adaptivity on page 1076	Configures an adaptivity timeout value, in minutes, for avoidance of channels detected with radar or high levels of interference
aeroscout on page 1077	Enables Aeroscout multicast packet forwarding
aggregation on page 1078	Configures 802.11n aggregation parameters
airtime-fairness on page 1082	Enables fair access for clients based on airtime usage
antenna-diversity on page 1083	Transmits antenna diversity for non-11n transmit rates
antenna-elevation on page 1083	Configures the antenna's elevation gain.
antenna-gain on page 1085	Specifies the antenna gain for the selected radio
antenna-mode on page 1086	Configures the radio antenna mode

Commands	Description
assoc-response on page 1087	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
association-list on page 1088	Associates an existing global association list with this radio interface
beacon on page 1099	Configures beacon parameters
bridge on page 1088	Configures client-bridge related parameters, if the selected radio's RF mode is set to bridge
channel on page 1100	Configures a radio's channel of operation
data-rates on page 1103	Specifies the 802.11 rates supported on a radio
description on page 1107	Configures the selected radio's description
dfs-rehome on page 1108	Reverts to configured home channel once *Dynamic Frequency Selection* (DFS) evacuation period expires
dynamic-chain-selection on page 1109	Enables automatic antenna mode selection
ekahau on page 1110	Enables Ekahau multicast packet forwarding
fallback-channel on page 1111	Configures the channel to which the radio switches in case of radar detection on the current channel
guard-interval on page 1112	Configures the 802.11n guard interval
ldpc on page 1113	Enables support for *Low Density Parity Check* (LDPC) on the radio interface
lock-rf-mode on page 1113	Retains user configured RF mode settings for the selected radio
max-clients on page 1114	Configures the maximum number of wireless clients allowed to associate with this radio
mu-mimo on page 1115	Enables multi-user multiple input multiple output (MU-MIMO) support on a radio
no (radio-interface-config-command) on page 1116	Negates or resets radio interface settings configures on a profile or a device
non-unicast on page 1119	Configures the handling of non unicast frames on this radio
off-channel-scan on page 1121	Enables selected radio's off channel scanning parameters
placement on page 1122	Defines selected radio's deployment location
power on page 1123	Configures the transmit power on this radio
preamble-short on page 1124	Enables the use of short preamble on this radio
probe-response on page 1125	Configures transmission parameters for probe response frames
radio-resource-measurement on page 1127	Enables 802.11k radio resource measurement
radio-share-mode on page 1128	Configures the mode of operation, for this radio, as radio-share
rf-mode on page 1129	Configures the radio's RF mode
rifs on page 1133	Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio
rts-threshold on page 1134	Configures the *Request to Send* (RTS) threshold value on this radio
shutdown on page 1135	Terminates or shuts down selected radio interface

Commands	Description
smart-rf on page 1136	Overrides Smart RF channel width setting on the selected radio interface
sniffer-redirect on page 1136	Captures and redirects packets to an IP address running a packet capture/analysis tool
stbc on page 1138	Configures radio's *Space Time Block Coding* (STBC) mode
transmit-beamforming on page 1138	Enables transmit beamforming on the selected radio interface
use on page 1139	Enables use of an association ACL policy and a radio QoS policy by selected radio interface
wips on page 1140	Enables access point to change its channel of operation in order to terminate rogue devices
wireless-client on page 1141	Configures wireless client parameters on selected radio
wlan on page 1142	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 1642 (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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
adaptivity [recovery|timeout <30-3600>]
```

Parameters

```
adaptivity [recovery|timeout <30-3600>]
```

adaptivity	Configures adaptivity parameters on the radio. These parameters are: recovery and timeout.
recovery	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.
timeout <30-3600>	Configures an adaptivity timeout • <30-3600> – Specify a value from 30 - 3600 minutes. The default is 90 minutes.

Example

```
nx9500-6C8809(config-profile-testAP505-if-radio1)#adaptivity timeout 200

nx9500-6C8809(config-profile-testAP505-if-radio1)#show context
 interface radio1
 adaptivity timeout 200
nx9500-6C8809(config-profile-testAP505-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

```
aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]
```

aeroscout	Enables Aeroscout packet forwarding and configures the packet forwarding parameters

forward ip <IP> port <0-65535>	Configures the following Aeroscout locationing engine details:
	• ip – Configures Aeroscout engine's IP address
	  • <IP> – 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.
	• port – Configures the port on which the Aeroscout engine is reachable
	  • <0-65535> – Specify the port number from 0 - 65535.

mac <MAC>	Configures the multicast MAC address to forward the Aeroscout packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format. The default value is 01-0C-CC-00-00-00.

Example

```
nx9500-6C8809(config-profile-ProfileTestAP505-if-radio2)#aeroscout forward ip
10.233.84.206 port 22

nx9500-6C8809(config-profile-ProfileTestAP505-if-radio2)#show context
 interface radio2
  aeroscout forward ip 10.233.84.206 port 22
nx9500-6C8809(config-profile-ProfileTestAP505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Disables Aeroscout packet forwarding

aggregation

interface-config-radio-instance on page 1072

Configures frame aggregation parameters. Frame aggregation is a IEEE 802.11e, 802.11n, and 802.11ac wireless networking standard. It increases throughput by sending two or more data frames in a single transmission. There are two types of frame aggregation: *Aggregate - MAC Service Data Unit* (A-MSDU) aggregation and *Aggregate - MAC Protocol Data Unit* (A-MPDU) aggregation. Both modes group several data frames into one large data frame.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
aggregation [ampdu|amsdu]
aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing|
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|128000|256000|
512000|1024000|default]
aggregation ampdu max-aggr-size tx <2000-1024000>
aggregation ampdu min-spacing [0|1|2|4|8|16|auto]
aggregation amsdu [rx-only|tx-rx]
```

Parameters

```
aggregation ampdu [rx-only|tx-only|tx-rx|none]
```

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU *(Aggregate MAC Protocol Data Unit)* frame aggregation parameters AMPDU aggregation joins multiple MPDU frames, addressed to a single destination, to form a single frame. It wraps each MPDU frame in a MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgment and retransmission of each aggregated data frame individually.
tx-only	Supports the transmission of AMPDU aggregated frames only
rx-only	Supports the receipt of AMPDU aggregated frames only
tx-rx	Supports the transmission and receipt of AMPDU aggregated frames (default setting)
none	Disables support for AMPDU aggregation

```
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535|128000|256000|
512000|1024000|default]
```

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation joins multiple MPDU frames, addressed to a single destination, to form a single frame. It wraps each MPDU frame in a MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgment and retransmission of each aggregated data frame individually.

max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit for transmitted and received packets.
rx [8191|16383|32767|65535|128000| 256000|512000| 1024000]	Configures the maximum limit (in bytes) advertised for received frame size • 8191 – Advertises a maximum frame size of 8191 bytes • 16383 – Advertises a maximum frame size of 16383 bytes • 32767 – Advertises a maximum frame size of 32767 bytes • 65535 – Advertises a maximum frame size of 65535 bytes • 128000 – Advertises a maximum frame size of 128000 bytes • 256000 – Advertises a maximum frame size of 256000 bytes • 512000 – Advertises a maximum frame size of 512000 bytes • 1024000 – Advertises a maximum frame size of 1024000 bytes (default setting) • default - Sets the default aggregation size.

```
aggregation ampdu max-aggr-size tx <2000-1024000>
```

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation joins multiple MPDU frames, addressed to a single destination, to form a single frame. It wraps each MPDU frame in a MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgment and retransmission of each aggregated data frame individually.

max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit for transmitted and received packets.
tx <2000-1024000>	Configures the maximum size (in bytes) for AMPDU aggregated transmitted frame size • <2000-1024000> – Sets the maximum aggregated transmitted frame size limit The available range depends on the AP type and the radio selected. For 802.11ac capable APs, the range is as follows: • radio 1 - 2000 - 65,535 bytes. The default value is 65,535 bytes. • radio 2 - The range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes. Note: For AP7662 and AP7632 models the range for radio 1 and radio 2 is 2000 - 1,024,000 bytes. And the default is 1,024,000 bytes. **Note:** The WiNG 802.11ac capable APs are: AP505, AP510, AP7522, AP7532, AP7562, AP7602, AP7612, AP7632, AP7662, AP8432, and AP8533. For non 802.11ac APs the range is as follows: • radio 1 and radio 2 - 2000 - 65,535 bytes. The default value is 65,535 bytes.

```
aggregation ampdu min-spacing [0|1|2|4|8|16|auto]
```

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation joins multiple MPDU frames, addressed to a single destination, to form a single frame. It wraps each MPDU frame in a MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgment and retransmission of each aggregated data frame individually.
min-spacing [0|1|2|4|8|16]	Configures the minimum gap, in microseconds, between AMPDU frames • 0 – Configures the minimum gap as 0 microseconds • 1 – Configures the minimum gap as 1 microseconds • 2 – Configures the minimum gap as 2 microseconds • 4 – Configures the minimum gap as 4 microseconds • 8 – Configures the minimum gap as 8 microseconds • 16 – Configures the minimum gap as 16 microseconds • auto – Auto configures the minimum gap depending on the platform and radio type (default setting)

```
aggregation amsdu [rx-only|tx-rx]
```

aggregation	Configures 802.11n frame aggregation parameters
amsdu	Configures AMSDU *(Aggregated MAC Service Data Unit)* 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.
rx-only	Supports the receipt of AMSDU aggregated frames only (default setting)
tx-rx	Supports the transmission and receipt of AMSDU aggregated frames

Example

```
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#aggregation ampdu tx-only

nx9500-6C8809(config-profile-505TestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

Parameters

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

airtime-fairness	Enables fair access to the medium for wireless clients based on their airtime usage
prefer-ht	Optional. Prioritizes high throughput (802.11n) clients over clients with slower throughput (802.11 a/b/g) and legacy clients
weight <1-10>	Optional. Configures the relative weightage for 11n clients over legacy clients. • <1-10> – Sets a weightage ratio for 11n clients from 1 - 10

Example

```
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#airtime-fairness prefer-ht weight 6

nx9500-6C8809(config-profile-505TestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
```

```
  airtime-fairness prefer-ht weight 6
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#
```

Related Commands

no on page 1055	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
antenna-diversity
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#antenna-diversity

nx9500-6C8809(config-profile-505TestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
nx9500-6C8809(config-profile-505TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Uses single antenna for non-11n transmit rates

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.

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:
```
ap510-133B38(config-device-94-9B-2C-13-3B-38-if-radio2)#service antenna-type dipole
```
2 Configure the antenna peak gain. For example:
```
ap510-133B38(config-device-94-9B-2C-13-3B-38-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:
```
ap510-133B38(config-device-94-9B-2C-13-3B-38-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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
antenna-elevation <-30.0-36.0>
```

Parameters

```
antenna-elevation <-30.0-36.0>
```

antenna-elevation <-30.0-36.0>	Configures the antenna elevation gain from -30.0 - 36.0 dB. Refer to the antenna specifications for antenna-elevation gain information. The default value is 0 dB.

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#antenna-elevation 5.0

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  antenna-elevation 5.0
  aggregation ampdu tx-only
  aeroscout forward ip 1.23.4.56 port 300
  antenna-diversity
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 PMACF *(Power Management Antenna Configuration File)* automatically configures the access point orwireless 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
antenna-gain <0.0-15.0>
```

Parameters

```
antenna-gain <0.0-15.0>
```

antenna-gain <0.0-15.0>	Sets the antenna gain from 0.0 - 15.0 dBi. The default is 0.00 dBi.

Usage Guidelines

Click here for more information on AP505 and AP510 radio and antenna specifications.

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#antenna-gain 12

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  antenna-elevation 5.0
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward ip 1.23.4.56 port 300
  antenna-diversity
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
antenna-mode [1*1|1*ALL|2*2|3*3|default]
```

Parameters

```
antenna-mode [1*1|1*ALL|2*2|default]
```

antenna-mode	Configures the antenna mode
1*1	Uses only antenna A to receive and transmit
1*ALL	Uses antenna A to transmit and receives on all antennas
2*2	Uses antennas A and C for both transmit and receive **Note:** AP505i, AP510i and AP560i are dual-radio access points, with eight internal antennas. The AP510e, is a dual-radio access point, with eight external antennas.
3*3	Uses antenna A, B, and C for both transmit and receive
default	Uses default antenna settings. This is the default setting.

Usage Guidelines

Note
For STBC feature support, the antenna-mode should not be configured to 1*1.

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#antenna-mode 2x2

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  antenna-elevation 5.0
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward ip 1.23.4.56 port 300
  antenna-mode 2x2
  antenna-diversity
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 that determine whether the access point ignores or responds to a client's association/authorization request

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
assoc-response [ac-strict|deny-threshold <1-12>|rssi-threshold <-128--40>]
```

Parameters

```
assoc-response [ac-strict|deny-threshold <1-12>|rssi-threshold <-128--40>]
```

assoc-response	Configures parameters based on which the AP ignores or responds to client's association/authorization request. The options are: ac-strict, deny-threshold, and rssi-threshold. **Note:** All three options are disabled by default.
ac-strict	Denies association requests from non 11ac capable wireless clients
deny-threshold <1-12>	Configures the number of times the AP ignores association/authorization requests, if the RSSI is below the configured RSSI threshold value • <1-12> – Specify a value from 1 - 12. **Note:** The AP always ignores association/authorization requests when deny-threshold is not specified and rssi-threshold is specified.
rssi-threshold <-128--40>	Configures the RSSI threshold. If the RSSI is lower than the threshold configured here, the AP ignores the association/authorization request. • <128--40> – Specify the RSSI threshold from -128 - -40 dBi.

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#assoc-response rssi-threshold -128
ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  antenna-elevation 5.0
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward ip 1.23.4.56 port 300
  antenna-mode 2x2
  antenna-diversity
  assoc-response rssi-threshold -128
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

Parameters

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

association-list global <GLOBAL-ASSOC-LIST-NAME>	Associates an existing global association list with this radio interface

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#association-list global test

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  antenna-elevation 5.0
  antenna-gain 12.0
  aggregation ampdu tx-only
  association-list global test
  aeroscout forward ip 1.23.4.56 port 300
  antenna-mode 2x2
  antenna-diversity
  assoc-response rssi-threshold -128
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Removes the global association list associated with this radio interface

bridge

interface-config-radio-instance on page 1072

Configures the *client-bridge* (CB) 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 — AP505, AP510, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP763, AP7662, AP8163, AP8543, AP8533

Note
WiNG 7.X.X does not support client-bridge functionality on the AP505, AP510 and AP560 model access points. This feature will be supported in future releases.

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 *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]]
```

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.
authentication-type [eap|none]	Configures the authentication framework used between the client-bridge and infrastructure WLAN APs. • eap – Uses EAP authentication (802.1X). • none – Uses no authentication. This is the default setting. Note: 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]
```

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 type [peap-mschapv2|tls]	If selecting EAP authentication, specify the EAP authentication type to use. The options are: • 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. Note: If selecting this option, use the following commands to configure the username and password: '`bridge > eap > username > <USER-NAME>`' '`bridge > eap > password > <PASSWORD>`' • TLS – Configures EAP authentication type as TLS. This mode uses trustpoints (TPs) to authenticate the CB AP and RADIUS server host. Note: If selecting this option, use the 'bridge > eap > trustpoint' command to configure the TPs used for authentication. Ensure that the authentication-type configured on the CB AP is the same as that on the infrastructure WLAN.

```
bridge eap username <USERNAME>
```

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 username <UESERNAME>	Configures username used for authentication with the RADIUS server host • <USERNAME> – Specify the username. Note: PEAP-MSCHAPv2 – For PEAP-MSCHAPv2 authentication. The username specified here should be configured in the RADIUS server policy used on the RADIUS server host. TLS – For TLS authentication, use the username configured in the CN field of the installed PKCS #12 client certificate.

```
bridge eap password <PASSWORD>
```

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 password [<PASSWORD>]	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. • password <PASSWORD> – Specify the password.

```
bridge eap trustpoint [client <TRUSTPOINT-NAME>|ca <TRUSTPOINT-NAME>]
```

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	If EAP authentication type is set to EAP-TLS, use this command to configure TP *(trustpoint)* details. In EAP-TLS authentication, the CB AP and RADIUS server host authenticate each other using TPs. A TP contains the *CA certificate* and the *CA-signed certificate authenticating* the device. To enable TP-based authentication, both the CB AP and the RADIUS server host must 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. Fo more information, see trustpoint (device-config-mode) on page 1300.
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 1846.

```
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>]]
```

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.
channel-dwell-time <50-2000>	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. • <50-2000> – Specify a value from 50 -2000 milliseconds. The default is 150 milliseconds.
channel-list [2.4GHz|5GHz] <LIST>	Configures the list of channels the radio scans when scanning for an infrastructure WLAN access point to associate • 2.4GHz <LIST> – Configures a list of channels for scanning across all the channels in the 2.4GHz radio band • 5GHz <LIST> – Configures a list of channels for scanning across all the channels in the 5.0 GHz radio band The following parameter is common to both of the 2.4 GHZ and 5.0 GHz bands: • <LIST> – Provide the list of channels separated by commas.
connect-through-bridges	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.
encryption-type [ccmp|none|tkip]	Configures the encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are: • ccmp – Uses WPA/WPA2 CCMP encryption • none – Uses no encryption method. This is the default setting. • tkip – Uses WPA/WPA2 TKIP encryption If using CCMP or TKIP, use the 'wpa2-wpa2' keyword to configure the pre-shared key (PSK).
inactivity-timeout <0-864000>	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. • <0-864000> – Specify a value from 0 - 864000 seconds. The default is 600 seconds.

keepalive [frame-type [null-data| wnmp]| interval <0-36000>]	Configures the keep-alive frame type and interval
	• frame-type – Configures the keepalive frame type exchanged between the client-bridge access point and the infrastructure access point/ controller. The options are:
	  • null-data – Transmits 802.11 NULL data frames. This is the default setting.
	  • wnmp – Transmits Wireless Network Management Protocol (WNMP) multicast packet
	• interval <0-36000> – Configures the interval, in seconds, between successive keep-alive frame transmission.
	  • <0-36000> – Specify a value from 0 - 36000 seconds. The default is 300 seconds.

max-clients <1-64>	Configures the maximum number of clients that the client-bridge AP can support • <1-14> – Specify a value from 1 - 64. The default is 64.
on-link-loss shutdown-other-radio <1-1800>	Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points is lost. • 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. • <1-1800> – 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.
on-link-up refresh-vlan-interface	Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points comes up. • 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.

roam-criteria [missed-beacons <1-60>| rssi-threshold <-128--40>]	Configures the following roaming criteria parameters
	• missed-beacons <1-60> – 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 s 20 seconds.
	  • <1-60> – Specify a value from 1 - 60 seconds. The default is 20 seconds.
	• rssi-threshold <-128--40> – Configures the minimum signal strength, received from target AP, for the bridge connection to be maintained before roaming
	  • <-128--40> – 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.

ssid <SSID>	Configures the infrastructure WLAN SSID the client bridge connects to • <SSID> – Specify the SSID.
wpa-wpa2 psk <LINE>	Configures the encryption PSKto use with the infrastructure WLAN • <LINE> – Enter the key Note: Pre-shared keys are valid only when the authentication-type is set to none and the encryption-type is set to tkip or ccmp. The PSK should be 8 - 32 characters in length.

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

no (radio-interface-config-command) on page 1116	Removes or resets this client-bridge settings

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 DTIM *(Delivery Traffic Indication Message)*. 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
beacon [dtim-period|period]
beacon dtim-period [<1-50>|bss <1-16> <1-50>]
beacon period [50|100|200]
```

Parametersd

```
beacon dtim-period [<1-50>|bss <1-8> <1-50>]
```

beacon	Configures radio beacon parameters
dtim-period	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.

<1-50>	Configures a single value to use on the radio. Specify a value between 1 and 50.
bss <1-16> <1-50>	Configures a separate DTIM for a BSS on this radio interface • <1-16> – Sets the BSS number from 1 - 16 • <1-50> – Sets the BSS DTIM from 1 - 50. The default is 2.

```
beacon period [50|100|200]
```

period [50|100|200]	Configures the beacon period (the interval between consecutive radio beacons) • 50 – Configures 50 K-uSec interval between beacons • 100 – Configures 100 K-uSec interval between beacons (default) • 200 – Configures 200 K-uSec interval between beacons

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)#beacon dtim-period bss 2 20
ap505-133E1C(config-profile-testap505-if-radio2)#beacon period 50

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  beacon dtim-period bss 9 2
  beacon dtim-period bss 10 2
  beacon dtim-period bss 11 2
  beacon dtim-period bss 12 2
  beacon dtim-period bss 13 2
  beacon dtim-period bss 14 2
  beacon dtim-period bss 15 2
  beacon dtim-period bss 16 2
  antenna-elevation 5.0
  antenna-gain 12.0
  aggregation ampdu tx-only
  association-list global test
  aeroscout forward ip 1.23.4.56 port 300
  antenna-mode 2x2
  antenna-diversity
  assoc-response rssi-threshold -128
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Removes the configured beacon parameters

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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
channel [smart|acs|random|ml-rrm|1|2|3|4|---------128www]
```

Parameters

```
channel [smart|acs|random|1|2|3|4|---------128www ]
```

channel	Configures a radio's channel of operation
[smart|acs|random||1|2|3|4|------128www]	Configures the radio's channel of operation, using one of the following options: • smart – Enables Smart RF the channel assignment for the selected radio (uses uniform spectrum spreading if Smart RF is not enabled). This is the default setting. • acs – Uses *automatic channel selection* (ACS) to assign a channel • random – Randomly assigns a channel • ml-rrm - Enables ml-rrm (Machine Learning - Radio Resource Management) to determine the channel assignment for the selected radio. The ML-RRM option provides an alternative solution to Smart RF management of radio settings, such as channel selection and transmit power. To use ML-RRM, you must first enable the ml-rrm agent in the access point's profile or device context. **Note:** ML-RRM can be enabled only on the WiNG AP7632 and AP7662 model access points and only if the APs are adopted to ExtremeCloud. **Note:** ExtremeAI can be enabled on the access point through the ExtremeCloud UI. For more information on ExtremeAI, please refer to the ExtremeAI User Guide available at https://extremenetworks.com/documentation. For more information on ExtremeAI, please refer to the ExtremeAI User Guide available at https://extremenetworks.com/documentation. • 1 – Sets channel 1 in 20 MHz mode as the selected radio's channel of operation • 2 – Sets channel 2 in 20 MHz mode as the selected radio's channel of operation • 3 – Sets channel 3 in 20 MHz mode as the selected radio's channel of operation

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#channel 1

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 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 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 — AP505i, AP510i, AP510e, AP560i, AP560h

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]
```

data-rates	Configures the 802.11 data rates on this radio
b-only	Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)
g-only	Uses rates that support operation in the 802.11g mode only (applicable for 2.4 and 4.9 GHz bands)
a-only	Uses rates that support operation in the 802.11a mode only (applicable for 5.0 GHz band only)
bg	Uses rates that support 802.11b and 802.11g wireless clients (applicable for 2.4 and 4.9 GHz bands)

bgn	Uses rates that support 802.11b, 802.11g, and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
gn	Uses rates that support 802.11g and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
an	Uses rates that support 802.11a and 802.11n wireless clients (applicable for 5.0 GHz band only)
default	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]
```

data-rates	Configures the 802.11 data rates on this radio
custom	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') • 1 – 1-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • 11 – 11-Mbps • 12 – 12-Mbps • 18 – 18-Mbps • 24 – 24-Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • mcs-1s – Applicable to 1-spatial stream data rates • mcs-2s – Applicable to 2-spatial stream data rates • mcs-3s – Applicable to 3-spatial stream data rates • basic-1 – Basic 1-Mbps • basic-2 – Basic 2-Mbps • basic-5.5 – Basic 5.5-Mbps • basic-6 – Basic 6-Mbps • basic-9 – Basic 9-Mbps • basic-11 – Basic 11-Mbps • basic-12 – Basic 12-Mbps • basic-18 – Basic 18-Mbps • basic-24 – Basic 24-Mbps • basic-36 – Basic 36-Mbps • basic-48 – Basic 48-Mbps • basic-54 – Basic 54-Mbps • basic-mcs-1s – Modulation and Coding Scheme data rates for 1 Spatial Stream **Note:** Refer to the Usage Guidelines Usage Guidelines (Supported data rates) on page 1105 section for 802.11an and 802.11ac MCS detailed dates rates for both with and without SGI *(short guard intervals)*.

```
data-rates mcs qam-only
```

data-rates	Configures the 802.11 data rates on this radio
mcs qam-only	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:

MCS-1Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
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:

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
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:

MCS-3Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
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-510TestProfile-if-radio1)#data-rates b-only

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets the 802.11 data rates on a radio
rf-mode on page 1129	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
description <WORD>
```

Parameters

```
description <WORD>
```

description <WORD>	Provide a description for the selected radio (should not exceed 64 characters in length).

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#description "Primary
radio to use"

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Removes a radio's description

dfs-rehome

interface-config-radio-instance on page 1072

Reverts to configured home channel once the DFS *(Dynamic Frequency Selection)* 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
dfs-rehome {holdtime <30-3600>}
```

Parameters

```
dfs-rehome {holdtime <30-3600>}
```

dfs-rehome {holdtime <30-3600>}	Enables the radio to revert to the configured home channel once the DFS evacuation period expires • holdtime – Optional. Specifies the duration, in minutes, to stay in the new channel • <30-3600> – Specify the holdtime from 30 - 3600 minutes. The default is 90 minutes.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#dfs-rehome holdtime 500

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  dfs-rehome holdtime 500
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Stays on DFS elected channel after evacuation period expires

dynamic-chain-selection

interface-config-radio-instance on page 1072

Enables dynamic chanin 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
dynamic-chain-selection {strict}
```

Parameters

```
dynamic-chain-selection {strict}
```

dynamic-chain-selection *{strict}*	Enables dynamic chain selection. • strict – Optional. Uses strict antenna-mode selection (single antenna for non-11n transmit rates)

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#dynamic-chain-selection
```

Related Commands

no (radio-interface-config-command) on page 1116	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 locationing maps, alerts and reports.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
ekahau [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

```
ekahau [forward ip <IP> port <0-65535>|mac <MAC>]
```

ekahau	Enables Ekahau multicast packet forwarding on this radio
forward ip <IP> port <0-65535>	Enables multicast packet forwarding to the Ekahau engine • ip <IP> – Configures the IP address of the Ekahau engine in the A.B.C.D format • port <0-65535> – Specifies the TZSP *(TaZman Sniffer Protocol)* port on Ekahau engine from 0 - 65535 TZSP is an encapsulation protocol, which is generally used to wrap 802.11 wireless packets.
mac <MAC>	Configures the multicast MAC address to forward the Ekahau multicast packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#ekahau forward ip 172.16.10.1 port
3

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Uses default Ekahau multicast MAC address

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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w.............74]
```

Parameters

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w.............74]
```

fallback-channel [100|100w|.....]	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. • [100|100w|100ww|...] – Select the fall back channel from the available options.

Example

```
nx9500-6C8809(config-profile-testAP510-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-testAP510-if-radio2)#show context
 interface radio2
  fallback-channel 104
nx9500-6C8809(config-profile-testAP510-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
guard-interval [any|long]
```

Parameters

```
guard-interval [any|long]
```

guard-interval	Configures the 802.11n guard interval
any	Enables the radio to use any short (400nSec) or long (800nSec) guard interval
long	Enables the use of long guard interval (800nSec). This is the default setting.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#guard-interval long

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
ldpc
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-Test510-if-radio1)#ldpc

nx9500-6C8809(config-profile-Test510-if-radio1)#show context
 interface radio1
  ldpc
nx9500-6C8809(config-profile-Test510-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
lock-rf-mode
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#lock-rf-mode

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
```

```
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
max-clients <0-512>
```

Parameters

```
max-clients <0-512>
```

max-clients <0-512>	Configures the maximum number of clients allowed to associate with a radio, subject to the access point's limit. Specify a value from 0 - 512. The default is 512. **Note:** For the WiNG 7.2.0 AP5XX model access points, the maximum number of clients supported per radio is 512. **Note:** For the WiNG 5.9.X legacy access points this range is 0 - 256 and the maximum number of clients supported per radio is 256.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#max-clients 100

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets the maximum number of wireless clients allowed to associate with a 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
mu-mimo
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-TestAP510-if-radio1)#mu-mimo
nx9500-6C8809(config-profile-TestAP510-if-radio1)#show context include-factory | include
mu-mimo
  mu-mimo
nx9500-6C8809(config-profile-TestAP510-if-radio1)#

ap510-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#mu-mimo

pa510-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#show context include-factory |
include mu-mimo
  mu-mimo
ap510-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Disables mu-mimo on the selected radio

no (radio-interface-config-command)

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 — AP505i, AP510i, AP510e, AP560i, AP560h

```
no <PARAMETERS>
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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.

Examples

```
nx9500-6C8809(config-profile-ap71xxTest-if-radio1)#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 radio1, 5GHz on radio2,
                          sensor on radio3)
rifs                      Configure Reduced Interframe Spacing (RIFS)
                          parameters
rts-threshold             Reset the RTS threshold to its default (65536)
rx-sensitivity-reduction  Configure radio receive sensitivity reduction
                          threshold
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-ap71xxTest-if-radio1)#
```

The following example shows radio interface settings before the ‘no’ commands are executed:

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  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-71xxTestProfile-if-radio1)#

nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no channel
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no antenna-gain
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no description
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no antenna-mode
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no beacon dtim-period
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#no beacon period
```

The following example shows radio interface settings after the ‘no’ commands are executed:

```
nx9500-6C8809(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  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-radio1)#
```

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 — AP505i, AP510i, AP510e, AP560i, AP560h

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]
```

non-unicast forwarding	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.
follow-dtim	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.
power-save-aware	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>]
```

non-unicast queue	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.
<1-200>	Specify a number from 1 - 200. This value applies to all BSSs. The default is 50 frames per BSS.
bss <1-16> <1-200>	Overrides the default on a specified BSS • <1-16> – Select the BSS number from 1 - 16. • <1-200> – Specify the number of broadcast packets queued for the selected BSS from 1 - 200.

```
non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]
```

non-unicast tx-rate	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.
bss <1-16>	Overrides the default on a specified BSS • <1-16> – 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.
dynamic-all	Dynamically selects a rate from all supported rates based on current traffic conditions
dynamic-basic	Dynamically selects a rate from all supported basic rates based on current traffic conditions
highest-basic	Uses the highest configured basic rate. This is the default setting.
lowest-basic	Uses the lowest configured basic rate

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#non-unicast queue bss 2 3

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#non-unicast tx-rate bss 1 dynamic-
all

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

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>}
```

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
channel-list [2.4GHz|5GHz]	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. • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<CHANNEL-LIST>	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>}
```

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
max-multicast <0-100>	Optional. Configures the maximum multicast/broadcast messages used to perform OCS • <0-100> – Specify a value from 0 - 100. The default is 4.
scan-interval <2-100>	Optional. Configures the scan interval in dtims • <2-100> – Specify a value from 2 - 100. The default is 20 dtims.

```
off-channel-scan {sniffer-redirect tzsp <IP>}
```

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
sniffer-redirect tzsp <IP>	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. • tzsp – Encapsulates captured packets in TZSP before redirecting to the specified host • <IP> – Specify the destination device IP address.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#off-channel-scan channel-list
2.4GHz 1

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
placement [indoor|outdoor]
```

Parameters

```
placement [indoor|outdoor]
```

placement	Defines the radio's location
indoor	Radio is deployed indoors (uses indoor regulatory rules). This is the default setting.
outdoor	Radio is deployed outdoors (uses outdoor regulatory rules)

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#placement outdoor

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets a radio's deployment location

power

interface-config-radio-instance on page 1072

Configures the selected radio's transmit power. Use this command to manually set the transmit power of the selected radio, or select the smart mode by which the transmit power is determined.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
power [<1-30>|smart]
```

Parameters

```
power [<1-30>|smart]
```

power	Configures the selected radio's transmit power
<1-30>	Configures the transmit power from 1 - 30 dBm (actual power could be lower based on regulatory restrictions) For APs with dual or three radios, use this option to manually configure each radio with a unique transmit power in respect to its intended client support function.
smart	Enables Smart RF to determine the optimum transmit power needed. Use this option to let Smart RF determine the selected radio's transmit power. If you are using this option for RF management, ensure that a Smart RF policy is configured and applied to the AP's RF Domain context. You can also use the default Smart RF policy. **Note:** By default, APs use Smart RF to determine transmit power.

Examples

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#power 12
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 (SpectraLink phones) require long preambles. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
preamble-short
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#preamble-short

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 sent by the access point in response to probe requests received from clients.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
probe-response [ac-strict|rate|retry|rssi-threshold]
probe-response ac-strict
probe-response retry
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
probe-response rssi-threshold <-128--40>
```

Parameters

```
probe-response ac-strict
```

probe-response ac-strict	Strictly restricts sending of probe-response frames to 802.11ac capable wireless clients. When enabled, the radio will only respond to probe-request frames received from 802.11ac capable clients.

```
probe-response retry
```

probe-response retry	Enables retransmission of probe-response frames if no acknowledgment is received from the client. This option is enabled by default.

```
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
```

probe-response rate	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.
follow-probe-request	Transmits probe responses at the same rate as the received request (default setting)
highest-basic	Uses the highest configured basic rate
lowest-basic	Uses the lowest configured basic rate

```
probe-response rssi-threshold <-128--40>
```

probe-response rssi-threshold <-128--40>	Ignores probe request from client if the received signal strength is less than the RSSI threshold specified here <-128--40> – Specify a value from -128 - -40.

Example

```
nx9500-6C8809(config-profile-testAP510-if-radio1)#probe-response rate highest-basic

nx9500-6C8809(config-profile-testAP510-if-radio1)#probe-response retry

nx9500-6C8809(config-profile-testAP510-if-radio1)#probe-response rssi-threshold -60

nx9500-6C8809(config-profile-testAP510-if-radio1)#show context
 interface radio1
  probe-response rate highest-basic
  probe-response rssi-threshold -60
nx9500-6C8809(config-profile-testAP510-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

Parameters

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

radio-resource-measurement	Enables 802.11k radio resource measurement on the radio
attenuation-threshold <1-199>	Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports • <1-199> – Specify the attenuation threshold from 1 -199. The default is 90.
max-entries <1-12>	Configures the maximum number of entries to include in channel and neighbor reports • <1-12> – Specify a value from 1 - 12. The default is 6.

Example

```
ap505-133E1C(config-profile-testap505-if-radio2)##radio-resource-measurement attenuation-
threshold 150

ap505-133E1C(config-profile-testap505-if-radio2)#radio-resource-measurement max-entries 10

ap505-133E1C(config-profile-testap505-if-radio2)#show context
 interface radio2
  mesh client
  beacon period 50
  antenna-elevation 5.0
  antenna-gain 12.0
  off-channel-scan
  aggregation ampdu tx-only
  association-list global test
  aeroscout forward ip 1.23.4.56 port 300
  antenna-mode 2x2
  antenna-diversity
  radio-resource-measurement max-entries 10
  radio-resource-measurement attenuation-threshold 150
  assoc-response rssi-threshold -128
  bridge ssid test
  mu-mimo
  ldpc
  lock-rf-mode
  fallback-channel 104
ap505-133E1C(config-profile-testap505-if-radio2)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
radio-share-mode [inline|off|promiscuous]
```

Parameters

```
radio-share-mode [inline|off|promiscuous]
```

radio-share-mode	Enables sharing of packets, switched by this radio, with the WIPS sensor module. There are two radio-share modes, these are: inline and promiscuous
inline	Enables sharing of all WLAN packets (matching the BSSID of the radio) serviced by the radio with the WIPS sensor module.
off	Disables radio share (no packets shared with the WIPS sensor module)
promiscuous	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-510TestProfile-if-radio1)#radio-share-mode promiscuous

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets the radio share mode for this radio to its default

rf-mode

interface-config-radio-instance on page 1072

Configures the radio's 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.

Set the mode to *sensor* if using the radio for rogue device detection.

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
rf-mode [2.4GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]
```

Parameters

```
rf-mode [2.4GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]
```

rf-mode	Configures the radio's mode of operation **Note:** For information on the software modes supported on AP5XX radios, see Usage Guidelines: Possible Combinations of RF Mode Configuration on page 1130.
2.4GHz-wlan	Provides WLAN service in the 2.4 GHz bandwidth
5GHz-wlan	Provides WLAN service in the 5.0 GHz bandwidth

scan-ahead	Enables this radio to operate as a scan-ahead mode A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does not support WLAN or mesh services. 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. 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. 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. Note: rf-mode scan-ahead is not supported on the AP 505i, AP510i/e, ap560i model access points.
bridge	Enables this radio to operate as client bridge that can authenticate and associate to a defined infrastructure Wireless LAN (WLAN) access point. Note: 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. Note: Client-bridge support is not enabled on AP505, AP510 and AP560 model access points.
sensor	Operates as a sensor radio. Configures this radio to function as a sensor, providing scanning services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services. Following is the sensor mode setting for the AP5XX: • AP505: both radio 1 and radio 2 must be configured as sensors. You cannot set one radio as sensor and the other radio for WLAN service. • AP5101/e, AP560i: Only radio 1 can be set as *sensor*. If setting radio 1 as Sensor, configure radio 2 as *5 GHz WLAN*. Note: For information on the software modes supported on AP5XX radios, see Usage Guidelines: Possible Combinations of RF Mode Configuration. Note: For information on AP510e radio and antenna configuration. see Usage Guidelines: AP510e Radio and Antenna Modes on page 1131

Usage Guidelines: Possible Combinations of RF Mode Configuration

Table 36: AP510i/e and AP560i/h Radio 1 and Radio 2: Software Modes

Software Mode 1	*Radio 1:*	Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths
	Radio 2:	Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz

Table 36: AP510i/e and AP560i/h Radio 1 and Radio 2: Software Modes (continued)

Software Mode 2	*Radio 1:*	Set to 2.4/5 GHz Sensor
	Radio 2:	Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 3 Note: Starting with the WiNG 7.2.0 release, SMART RF is supported on AP510i/e and AP560i/h model access points running in the dual-5GHz mode.	*Radio 1:*	Set to 5 GHz, Channels 36 - 64 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths
	Radio 2:	Set to 5 GHz, Channels 100 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz bandwidths

Note
The AP510e and AP510i/h have the same hardware specifications with one basic difference, AP510e has eight, *external* antennas, whereas, AP510i/h has eight, *internal* antenna ports.

Note
The AP560h supports the following two antenna types: 30 degree and 70 degree. Whereas, the AP560i supports only a single omni-directional antenna type on all eight antenna ports.

Table 37: AP505i Radio 1 and Radio 2: Software Modes

Software Mode 1	*Radio 1:*	Set to 2.4 GHz WLAN, Channels 1 - 11 in the 20 MHz /40 MHz bandwidths
	Radio 2:	Set to 5 GHz WLAN, Channels 36 - 165 in the 20 MHz /40 MHz /80 MHz /160 MHz
Software Mode 2	*Radio 1:*	Set to Sensor.
	Radio 2:	Set to Sensor.

Usage Guidelines: AP510e Radio and Antenna Modes

Note
The AP510e and AP510i are dual-radio APs with one basic difference, AP510e has eight, *external* antennas. Whereas, AP510i has eight, *internal* antennas.

The following table lists the external antenna configurations required to support the different software modes on the AP510e model access point.

Table 38: AP510e: External Antenna Configurations

	Antenna Ports	
Software Mode	**2.4/5G Antennas: 1, 2, 3, 4**	**5G Antennas: 5, 6, 7, 8**

Table 38: AP510e: External Antenna Configurations (continued)

Mode 1 • Radio 1 - 2.4 GHz WLAN • Radio 2 - 5 GHz WLAN Note: This mode requires only *FOUR, dual-band* antennas connected to ANT sockets 1 to 4.	Dual-band 2.4 GHz/5 GHz	None
Mode 2 • Radio 1 - 2.4/5 GHz Sensor • Radio 2 - 5 GHz WLAN Note: This mode requires *FOUR, dual-band* antennas connected to ANT sockets 1 to 4, and *FOUR, 5G-band* antennas connected to ANT sockets 5 to 8.	Dual-band 2.4 GHz/5 GHz	5 GHz
Mode 3 • Radio 1 - 5 GHz WLAN • Radio 2 - 5 GHz WLAN Note: Requires *FOUR, 5G-band* antennas connected to ANT sockets 1 to 4, and *FOUR, 5G-band* antennas connected to ANT sockets 5 to 8.	5 GHz	5 GHz

Note

To enable the AP510e radio, you *must* map a WLAN to the AP radio and *also* configure the antenna-id for the group-1 (1 to 4) or group-2 (5 to 8) antennas. For *Software Mode 1*, only group-1 antenna-id needs to be configured, since, in this mode the 5G, 5 - 8 antennas are not used. For *Software Mode 2* and *Software Mode 3* both *group-1* and *group-2* antenna-ids need to be configured, since both sets of antennas are used. For information on configuring the antenna-id, see antenna-id (ap510e) on page 861.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#rf-mode sensor

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
ap505-134006(config-device-94-9B-2C-13-40-06-if-radio1)#rf-mode 2.4GHz-wlan
ap505-134006(config-device-94-9B-2C-13-40-06-if-radio2)#rf-mode 5GHZ-Wlan
ap505-13403B(config-device-94-9B-2C-13-40-38-if-radio1)#wlan wlan123 bss 1 primary
ap505-13403B(config-device-94-9B-2C-13-40-38-if-radio2)#wlan wlan123 bss 1 primary
ap505-134006(config-device-94-9B-2C-13-40-06)#show cont
ap505 94-9B-2C-13-40-06
use profile default-ap505
use rf-domain default
hostname ap505-134006
interface radio1
  channel 1
  wlan wlan123 bss 1 primary
interface radio2
  channel 36
  wlan wlan123 bss 1 primary
no adoption-mode
ap505-134006(config-device-94-9B-2C-13-40-06)#..
ap505-134006(config)#commit wr mem
[OK]
ap505-134006(config)#show wi rad
-------------------------------------------------------------------------------------
RADIO              RADIO-MAC             RF-MODE    STATE   CHANNEL   POWER  #CLIENT
-------------------------------------------------------------------------------------
ap505-134006:R1    94-9B-2C-0E-88-80 2.4GHz-wlan     On   1 (    1)  14 (smt)  1
ap505-134006:R2    94-9B-2C-0E-88-90   5GHz-wlan     On   36 (   36) 16 (smt)  1
-------------------------------------------------------------------------------------
Total number of radios displayed: 2
ap505-134006(config)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets the radio's mode of operation
data-rates on page 1103	Configures the 802.11 data rates on this radio

rifs

interface-config-radio-instance on page 1072

Configures RIFS *(Reduced Interframe Spacing)* 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
rifs [none|rx-only|tx-only|tx-rx]
```

Parameters

```
rifs [none|rx-only|tx-only|tx-rx]
```

rifs	Configures RIFS parameters
none	Disables support for RIFS. Consider setting the value to None for high-priority traffic to reduce packet delay.
rx-only	Supports RIFS possession only
tx-only	Supports RIFS transmission only
tx-rx	Supports both RIFS transmission and possession (default setting)

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#rifs tx-only

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Disables radio's RIFS parameters

rts-threshold

interface-config-radio-instance on page 1072

Configures the RTS *(Request to Send)* threshold value on this radio

RTS is a transmitting station's signal that requests a CTS *(Clear To Send)* 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
rts-threshold <0-65536>
```

Parameters

```
rts-threshold <0-65536>
```

rts-threshold <0-65536>	Specify the RTS threshold value from 0 - 65536 bytes. The default is 65536 bytes.

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#rts-threshold 100

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Resets a radio's RTS threshold to its default

shutdown

interface-config-radio-instance on page 1072

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
shutdown
```

Parameters

```
None
```

Example

```
ap505-133E1C(config-profile-test510-if-radio1)#shutdown
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
smart-rf preferred-channel-width [20MHz|40MHz|80MHz]
```

Parameters

```
smart-rf preferred-channel-width [20MHz|40MHz|80MHz]
```

smart-rf preferred-channel-width [20MHz| 40MHz|80MHz]	Configures the preferred channel width. The options are: • 20MHz – Sets 20 MHz as the preferred channel of operation • 40MHz – Sets 40MHz as the preferred channel of operation • 80MHz – Sets 80MHz as the preferred channel of operation (default setting)

Example

```
nx9500-6C8809(config-profile-testAP510-if-radio1)#smart-rf preferred-channel-width 40MHz

nx9500-6C8809(config-profile-testAP510-if-radio1)#show context
 interface radio1
  smart-rf preferred-channel-width 40MHz
  rate-selection opportunistic
nx9500-6C8809(config-profile-testAP510-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

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)}
```

sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool
omnipeek	Encapsulates captured packets in proprietary header (used with OmniPeek and plug-in)
tzsp	Encapsulates captured packets in TZSP (used with WireShark and other tools)
<IP>	Specify the IP address of the device running the capture/analysis tool (the host to which captured off channel scan packets are redirected)
[1|10|100|100w ----------]	Specify the channel to capture packets • 1 – Channel 1 in 20 MHz mode (default setting) • 10 – Channel 10 in 20 MHz mode • 100 – Channel 100 in 20 MHz mode • 100w – Channels 100w in 40 MHz mode (channels 100*,104)
snap <1-65535>	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. • <1-65535> – Specify the maximum truncated byte length of captured packets.
append descriptor	Optional – Enables appending of the radio's receive descriptor to the captured packet

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#sniffer-redirect omnipeek
172.16.10.1 channel 1

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Disables packet capture and redirection

stbc

interface-config-radio-instance on page 1072

Configures the radio's STBC *(Space Time Block Coding)* 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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
stbc [auto|none|tx-only]
```

Parameters

```
stbc [auto|none|tx-only]
```

stbc	Configures the radio's STBC mode
auto	Autoselects STBC settings based on the platform type and other radio interface settings. This is the default setting.
none	Disables STBC support
tx-only	Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#stbc tx-only

rfs6000-37FABE(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  stbc tx-only
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
transmit-beamforming
```

Parameters

```
None
```

Example

```
nx9500-6C8809(config-profile-testAP510-if-radio1)#transmit-beamforming
```

Related Commands

no (radio-interface-config-command) on page 1116	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 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 — AP505i, AP510i, AP510e, AP560i, AP560h

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>]
```

use	Applies an association ACL policy and a radio QoS policy on this radio interface
association-acl-policy	Uses a specified association ACL policy with this radio interface • <ASSOC-ACL-POLICY-NAME> – Specify the association ACL policy name (should be existing and fully configured).
radio-qos-policy	Uses a specified radio QoS policy with this radio interface • <RADIO-QoS-POLICY-NAME> – Specify the radio QoS policy name (should be existing and fully configured).

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#use association-acl-policy test

nx9500-6C8809(config-profile-510TestProfile-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
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Note

WiNG access points use Smart RF to perform off-channel scans. Therefore, ensure that a Smart RF policy is configured and applied to the access points RF Domains to enable them perform rogue detection and termination.

Syntax

```
wips airtime-termination [allow-channel-change|spectrum-management-strict]
```

Parameters

```
wips airtime-termination [allow-channel-change|spectrum-management-strict]
```

wips airtime-termination allow-channel-change	Enables access point to change its channel of operation (to that of the rogue device) in order to terminate the rogue device
spectrum-management-strict	Enables the processing of spectrum management capability of an AP before performing air-termination

Example

```
nx9500-6C8809(config-profile-testAP510-if-radio1)#wips air-termination allow-channel-change
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

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>
```

wireless-client	Configures wireless client parameters
tx-power <0-20>	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. • <0-20> – Specify transmit power from 0 - 20 dBm.

```
wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]
```

wireless-client	Configures wireless client parameters

tx-power [802.11d|wing-ie]	Configures the transmit power indicated to wireless clients
	• 802.11d – Advertises in the IEEE 802.11d country information element
	  • wing-ie – Optional. Advertises in the WiNG information element (173)
	• wing-ie – Advertises in the WiNG information element (173). This is the default setting.
	  • 802.11d – Optional. Advertises in the IEEE 802.11d country information element

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#wireless-client tx-power 20

nx9500-6C8809(config-profile-510TestProfile-if-radio1)#show context
 interface radio1
  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-510TestProfile-if-radio1)#
```

Related Commands

no (radio-interface-config-command) on page 1116	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 — AP505i, AP510i, AP510e, AP560i, AP560h

Syntax

```
wlan <WLAN-NAME> {bss|primary}
wlan <WLAN-NAME> {bss <1-16>} {primary}
```

Parameters

```
wlan <WLAN-NAME> {bss <1-16>} {primary}
```

<WLAN-NAME> {bss <1-16> | primary}	Specify the WLAN name (it must have been already created and configured) • bss <1-16> – Optional. Specifies a BSS for the radio to map the WLAN • <1-18> – Specify the BSS number from 1 - 16. primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS • primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS

Example

```
nx9500-6C8809(config-profile-510TestProfile-if-radio1)#wlan TestWLAN primary

nx9500-6C8809(config-profile-510TestProfile-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-510TestProfile-if-radio1)#
ap505-134006(config-device-94-9B-2C-13-40-06-if-radio1)#rf-mode 2.4GHz-wlan
ap505-134006(config-device-94-9B-2C-13-40-06-if-radio2)#rf-mode 5GHZ-Wlan
ap505-13403B(config-device-94-9B-2C-13-40-38-if-radio1)#wlan wlan123 bss 1 primary
ap505-13403B(config-device-94-9B-2C-13-40-38-if-radio2)#wlan wlan123 bss 1 primary
ap505-134006(config-device-94-9B-2C-13-40-06)#show cont
ap505 94-9B-2C-13-40-06
use profile default-ap505
use rf-domain default
hostname ap505-134006
interface radio1
  channel 1
  wlan wlan123 bss 1 primary
interface radio2
  channel 36
  wlan wlan123 bss 1 primary
no adoption-mode
ap505-134006(config-device-94-9B-2C-13-40-06)#..
ap505-134006(config)#commit wr mem
[OK]
ap505-134006(config)#show wi rad
-------------------------------------------------------------------------------------
RADIO              RADIO-MAC             RF-MODE    STATE   CHANNEL   POWER  #CLIENT
-------------------------------------------------------------------------------------
ap505-134006:R1    94-9B-2C-0E-88-80 2.4GHz-wlan     On   1 (    1)  14 (smt)  1
ap505-134006:R2    94-9B-2C-0E-88-90   5GHz-wlan     On   36 (   36) 16 (smt)  1
-------------------------------------------------------------------------------------
```

```
Total number of radios displayed: 2
ap505-134006(config)#
```

Related Commands

no (radio-interface-config-command) on page 1116	Disables a WLAN on a radio

interface-config-wwan-instance

interface on page 1009

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
apn on page 1145	Configures the access point's name provided by the service provider
auth-type on page 1145	Configures the authentication types used on this interface
crypto on page 1146	Associates a crypto map with this interface
ip on page 1147	Associates an IP ACL with this interface
no on page 1148	Removes or reverts the WWAN interface settings
password on page 1149	Configures a password for this WWAN interface
use on page 1150	Associates an IP ACL with this interface
username on page 1151	Configures the names of users accessing this interface

apn

interface-config-wwan-instance on page 1144

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>
```

apn <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

no on page 1148	Removes the configured access point name.

auth-type

interface-config-wwan-instance on page 1144

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]
```

auth-type	Configures the authentication protocol used on this interface. The options are: PAP, CHAP, MSCHAP, and MSCHAP-v2
chap	Configures Challenge-Handshake Authentication Protocol (CHAP). This is the default value.
mschap	Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP)
mschapv2	Configures Microsoft Challenge-Handshake Authentication Protocol (MSCHAP) version 2
pap	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

no on page 1148	Removes the authentication protocol configured on this interface

crypto

interface-config-wwan-instance on page 1144

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>
```

crypto map <CRYPTO-MAP-NAME>	Associates a crypto map with this interface • <CRYPTO-MAP-NAME> – Specify the crypto map name (should be existing and configured).

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

no on page 1148	Removes the crypto map associated with this interface

ip

interface-config-wwan-instance on page 1144

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>
```

ip	Configures IP related settings on this interface
default-gateway priority <1-8000>	Configures the default-gateway's (learned by the wireless WAN) priority. • <1-8000> – Specify a value from 1 - 8000. The default is 3000.

```
ip nat [inside|outside]
```

ip	Configures IP related settings on this interface
nat [inside|outside]	Configures the NAT settings. This option is disabled by default. • 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. • 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.

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

no on page 1148	Removes IP related settings on this interface

no

interface-config-wwan-instance on page 1144

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>
```

no <PARAMETERS>	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 1144

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>]
```

password	Configures a password for this WWAN interface
2 <WORD>	Configures an encrypted password. Use this option when copy pasting the password from another device.
<WORD>	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

no on page 1148	Removes the configured password

shutdown

interface-config-wwan-instance on page 1144

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

no on page 1148	Re-starts the WWAN interface

use

interface-config-wwan-instance on page 1144

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>
```

use ip-access-list in <ACCESS-LIST-NAME>	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. • <ACCESS-LIST-NAME> – Specify the IP ACL name.

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 1148	Removes the IP ACL associated with this interface

username

interface-config-wwan-instance on page 1144

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>
```

username <WORD>	Configures the username for authentication support by the cellular data carrier • <WORD> – Specify the username (should not exceed 32 characters).

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

no on page 1148	Removes the configured username

interface-config-bluetooth-instance

interface on page 1009

WiNG access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. Both *Bluetooth classic* and *Bluetooth low energy* (BLE) technology are supported. Bluetooth classic-enabled radios 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.

WiNG model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio periodically sends non-connectable, undirected LE *(low-energy)* advertisement packets. 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.

Supported in the following platforms:

- Access Points – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, AP7632, AP7662, AP8432, AP8533

To switch to this mode, use the following commands in the AP's profile or device context:

```
<DEVICE>(config)#profile <ap-type> <PROFILE-NAME>

<DEVICE>(config-profile-default-ap-type)#interface bluetooth ?
  <1-1>  Bluetooth interface index?
```

The following example uses the default-ap505 profile instance to configure the Bluetooth radio interface:

```
nx9500-6C8809(config-profile-default-ap505)#interface bluetooth 1
nx9500-6C8809(config-profile-default-ap505-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 opreation mode
  no           Negate a command or set its defaults
  shutdown     Shutdown the selected bluetooth radio interface
  tron         Tron-tracking

  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-ap505-if-bluetooth1)
```

Commands	Description
beacon on page 1153	Configures the Bluetooth radio's beacon's emitted transmission pattern
description on page 1156	Configures a description for the Bluetooth radio interface
eddystone on page 1156	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'.
ibeacon on page 1157	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'.
mode on page 1159	Configures the Bluetooth radio's mode of operation
shutdown on page 1160	Shutdowns the selected Bluetooth radio interface
tron on page 1161	Configures parameters that enable TRON tracking and reporting on this Bluetooth radio **Note:** Tron tracking is not
no (bluetooth-inf-config-command) on page 1166	Removes or reverts to default this Bluetooth radio interface's settings

beacon

interface-config-bluetooth-instance on page 1152

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 – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, AP7632, AP7662, AP8432, AP8533

Syntax

```
beacon [pattern|period|txpower]

beacon pattern [eddystone-url1|eddystone-ulr2|ibeacon]

beacon period <100-10000>
beacon txpower <-15-6>
beacon txpower <-15-31>
```

Parameters

```
beacon pattern [eddystone-url1|eddystone-ulr2|ibeacon]
```

beacon pattern [eddystone-url1| eddystone-ulr2| ibeacon]	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: • eddystone-url1 – Transmits an Eddystone-URL beacon using URL 1. This is the default setting. • eddystone-url2 – Transmits an Eddystone-URL beacon using URL 2 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 'eddystone-url1' or 'eddystone-ulr2', use the 'eddystone' keyword to configure Eddystone beacon payload parameters. For more information, see eddystone on page 1156. • 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 ibeacon on page 1157. For more information on configuring the Bluetooth radio's operational mode, see mode on page 1159.

```
beacon period <100-10000>
```

beacon period <100-10000>	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). • <100-10000> – Specify a value from 100 - 10000 milliseconds. The default value is 1000 milliseconds.

```
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 to 6 dBM. The default value is -10 dBm. **Note:** The transmit power range of -15 to 6 is applicable for the following APs: AP7612, AP7622, AP7602, AP8432, AP8533

```
beacon txpower <-15-31>
```

beacon txpower <-15-31>	Configures the Bluetooth radio's le-beacon transmit power. This determines how far a beacon can transmit data. • <-15-31 – Specify a value from -15 to 31 dBM. The default value is -10 dBm. Note: The transmit power range of -15 to 6 is applicable for the following APs: AP7632, AP7662, AP5XX

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-Radio1
  mode le-beacon
  beacon pattern eddystone-url2
  beacon period 900
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Configurations enabling IoT on AP5XX IoT:

```
ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#mode le-beacon

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#beacon txpower 31

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#beacon period 100
```

Enable the interface

```
ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#no shutdown
```

AP5XX ibeacon configurations:

```
ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#beacon pattern ibeacon

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#ibeacon major 0

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#ibeacon minor 65535

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#ibeacon uuid
123456789A123456789A123456789ABC

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#ibeacon calibration rssi 1
```

AP5XX eddystone configuration

```
ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#mode le-beacon

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#beacon pattern eddystone url1

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#eddystone url 1 http://
www.ap510test.com

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#eddystone calibration rssi 2
```

Related Commands

no (bluetooth-inf-config-command) on page 1166	Removes or reverts to default this Bluetooth radio's beacon-related configurations

description

interface-config-bluetooth-instance on page 1152

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 – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, 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-Radio1

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  description AP8432-BLE-Radio1
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no (bluetooth-inf-config-command) on page 1166	Removes this Bluetooth radio interface's description

eddystone

interface-config-bluetooth-instance on page 1152

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-ulr2'.

Supported in the following platforms:

- Access Points – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, AP7632, AP7662, AP8432, AP8533

Syntax

```
eddystone [calibration-rssi <-127-127>|url [1|2] <WORD>]
```

Parameters

```
eddystone [calibration-rssi|url [1|2] <WORD>]
```

eddystone [calibration-rssi <-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 to 127 dBm. The default value is -19 dBm. • url [1|2] <WORD> – Configures the Eddystone URL 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-Radio1
  mode le-beacon
  beacon pattern eddystone-url2
  beacon period 900
  eddystone calibration-rssi -120
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

For AP5XX IoT configuration, see Configurations enabling IoT on AP5XX IoT.

Related Commands

no (bluetooth-inf-config-command) on page 1166	Removes or reverts to default this Bluetooth radio's Eddystone beacon payload configurations

ibeacon

interface-config-bluetooth-instance on page 1152

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 – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, 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>]
```

ibeacon	Configures following iBeacon beacon payload parameters: calibration-rssi, major, minor, and uuid
calibration-rssi <-127-127>	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. • <-127-127> – Specify a value from -127 to 127 dBm. The default value is -60 dBm.
major <0-65535>	Configures the iBeacon Major value that identifies a subset of beacons within the larger set. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. • <0-65535> – Specify a value from 0 - 65535. The default value is 1111.
minor <0-65535>	Configures the iBeacon Minor value that precisely pinpoints beacon location. Minor values help identify individual beacons within a group of beacons assigned a major value. This value complements the UUID and Major values to provide more granular identification of a specific location, such as a particular shelf, door-way, or item • <0-65535> – Specify a value from 0 - 65535. The default value is 2222.
uuid <WORD>	Configures an identifier that differentiates a large group of related beacons. 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. • <WORD> – Specify the UUID (should not exceed 32 hexadecimal characters). The default value is 01F101F101F101F101F101F101F101F1.

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)#
```

For AP5XX IoT configuration, see Configurations enabling IoT on AP5XX IoT.

Related Commands

no (bluetooth-inf-config-command) on page 1166	Removes or reverts to default this Bluetooth radio's iBeacon beacon payload parameters

mode

interface-config-bluetooth-instance on page 1152

Configures the Bluetooth radio's mode of operation as bt-sensor, le-beacon, le-sensor, or tron-tracking.

Supported in the following platforms:

- Access Points – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, AP7632, AP7662, AP8432, AP8533

Syntax

```
mode [bt-sensor|le-beacon|le-sensor|tron-tracking]
```

Parameters

```
mode [bt-sensor|le-beacon|le-sensor|tron-tracking]
```

mode	Configures the Bluetooth radio's mode of operation. The options are: • bt-sensor – 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. • le-beacon – 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 beacon on page 1153 keyword to configure the Beacon transmission period and Beacon transmission pattern. • le-sensor – 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 ExtremeLocation server or a third-party locationing server). • tron-tracking – TRON is a proprietary FedEx feature. Select this option to enable TRON tracking. When enabled, it BLE-enabled, WiNG APs detect 'ID Nodes' within a managed network and report to a proprietary FedEx back-end server application. If selecting this option, configure the Bluetooth radio's initial configurations needed to enable TRON tracking and reporting. For more information, see tron on page 1161. Note: Tron-tracking is only supported on AP8533 model access point.

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)#

ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1 )#mode le-beacon
```

For AP5XX IoT configuration, see Configurations enabling IoT on AP5XX IoT.

Related Commands

no (bluetooth-inf-config-command) on page 1166	Reverts this Bluetooth radio's mode of operation to le-beacon

shutdown

interface-config-bluetooth-instance on page 1152

Shutsdown the selected Bluetooth radio interface

Note
The `no → shutdown` command enables the BLE interface.

Supported in the following platforms:

- Access Points – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, 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)#
ap510-133A75#(config-device-94-9B-2C-13-3A-75-if-bluetooth1)#no shutdown
```

For AP5XX IoT configuration, see Configurations enabling IoT on AP5XX IoT.

Related Commands

no (bluetooth-inf-config-command) on page 1166	Reverses shutdown

tron

interface-config-bluetooth-instance on page 1152

Sets the configurations required by TRON-capable, WiNG APs to start TRON-tracking and reporting.

Note
WiNG 'TRON' is a licensed feature, designed specifically for FedEX. The 'TRON' license can be applied on the NX5500, NX7500, NX9500, NX9600, and VX900 platforms.

TRON is a proprietary FedEx BLE asset tracking application that tracks tagged packages moving through a distribution center. It is a multi-tier application consisting of the following elements:

- The “ID Nodes” – These are small, battery-powered BLE *(Bluetooth Low Energy)* devices attached to FedEx packages. Each ID Node (also called tag) is uniquely identified by its Bluetooth device

address. The ID Node sends out BLE advertisements, with a payload containing information about the state and configuration of the ID Node.

- The FMN *(Fixed Master Node)* – This is a functionality running on the TRON-capable, WiNG AP. The FMN listens for BLE advertisements beaconed by the ID Nodes. When the FMN senses an ID Node, it records the state and condition of the ID Node in an internal table. At regular intervals, the FMN reviews this table and reports interesting information about the ID Nodes to the FedEx backend server.

  The FMN also connects to an ID Node to read/write arbitrary GATT *(Generic Attribute Profile)* attributes, as instructed by the back-end server.

  Each TRON-capable, WiNG AP will be able to track up to 2000 ID Nodes at a time.
- The FedEx backend provisioning server – This is a FedEx proprietary application that tracks the ID Nodes based on the information sent to it by the FMN running on the WiNGAP.
- The MQTT *(Message Queuing Telemetry Transport)* Broker– MQTT is a standard publish-subscribe-based messaging protocol, which allows clients to exchange messages through an intermediate component, called the broker, A client (the publisher) publishes messages on a particular “topic” to the MQTT Broker, which filters these messages and forwards them correctly to other clients (the subscribers) that have subscribed to that “topic”.

  All communication between the FMN and the backend server is through the MQTT Broker. The FMN and FedEx backend server are the clients (publisher and subscriber) of the MQTT Broker. They communicate by publishing/subscribing to topics they have agreed upon in advance. The FMN and server can publish as well as subscribe messages on the pre-defined topics

To enable TRON tracking, you will need a controller with the TRON license applied, TRON-capable APs adopted to this controller. However, to TURN ON the TRON capabilities on a WiNG AP, the following two things are needed:

- The adopting controller must explicitly ‘give permission’ to the AP to enable the TRON feature. For this, the controller must have the TRON license applied on it. For more information on applying the TRON license, see license on page 1280.
- The AP should have the ‘initial configurations’ set in its Bluetooth interface context. Use this command to set these initial configurations.

Note

Before setting the initial configurations, set the AP’s bluetooth radio *mode* to *tron-tracking*. For more information, see mode on page 1159.

Supported in the following platforms

- Access Points – AP-8533

Syntax

```
tron [delete-operating-config-on-start|ignore-mqtt-truststore|initial-config|
reconstruct-nodetype-db-on-start]

tron delete-operating-config-on-start

tron ignore-mqtt-truststore

tron initial-config mqtt [client-prefix <WORD>|password <WORD>|port <1025-65535>|
server [<IP>|<HOST-NAME>]|topic-publish-prefix <LINE>|topic-subscribe-prefix <LINE>|
username <WORD>]

tron reconstruct-nodetype-db-on-start
```

Parameters

```
tron delete-operating-config-on-start
```

tron delete-operating-config-on-start	Enables the TRON software, on the AP, to delete the TRON “operating configuration” before starting any other TRON operations. Issue this command only if you wish to reload the operating configuration from the provisioning server. When the TRON software on an AP comes up for the first time, it uses the "initial-configuration" to connect with the backend provisioning server and download the operating configuration. This operating configuration is stored in the AP's file system. The configuration persists across TRON enables/disables and across AP reboots. In case the "operating configuration" has been misconfigured, the only means to delete it is by using this command. When issued, the command deletes the operating configuration. After the deletion, the AP's uses the “initial configuration” to connect to the provisioning server through the MQTT broker and download the operating configuration. However, if you execute this command while the TRON software is already up and running, it will have no effect until you restart the TRON. **Note:** Once the TRON software has obtained a new operating configuration and reconnected to the MQTT Broker, issue the `no → tron delete-operating-config-on-start` command to retain the new operating configuration across reboots and enable/disable operations. **Note:** To view the operating configuration, execute the `show → tron → operating-configuration → {on <AP-NAME>}` command. For more information, see tron (show command) on page 812.

```
tron ignore-mqtt-truststore
```

tron ignore-mqtt-truststore	Enable this option to force the MQTT functionality on the AP to use URIs beginning with *tcp:* and not *ssl:* When enabled, the TRON software, on starting up, ignores existing MQTT truststore (aka, certificate file), and uses a URI that begins with *tcp:* instead of *ssl:* **Note:** However, if you execute this command while the TRON software is already up and running, it will have no effect until you restart the TRON. This parameter is not mandatory, and is disabled by default.

```
tron initial-config mqtt [client-prefix <WORD>|password <WORD>|port <1025-65535>|
server [<IP>|<HOST-NAME>]|topic-publish-prefix <LINE>|topic-subscribe-prefix <LINE>|
username <WORD>]
```

tron initial-config mqtt	Sets the initial configurations required by the TRON-capable, WiNG AP to recognize and associate with the MQTT Broker for the first time. After associating with the Broker, the FMN functionality on the WiNG AP begins exchanging messages with the FedEx backend server. This FedEx backend server downloads an operating configuration to the AP. Note: The initial configurations are mandatory. However, once the AP is provisioned with the FedEx proprietary operating configuration, the initial configuration is ignored. To view the operating configuration, execute the `show → tron → operating-configuration → {on <AP-NAME>}` command. For more information, see tron (show command) on page 812. Note: The FMN also connects to an ID Node to read/write arbitrary GATT attributes, as instructed by the back-end server.
client-prefix <WORD>	Configures the MQTT client's prefix • <WORD> – Provide the prefix (should not exceed 16 characters in length). Note: The default value is 'FMN'.
password <WORD>	Configures the password required to authenticate with the MQTT Broker. You will need a username/password combination in order for the FMN to authenticate and associate with the MQTT Broker. Use the 'username' and 'password' options to specify the username and password respectively. • <WORD> – Specify the password either as clear text or as encrypted text. In case of clear text, the password should not exceed 32 characters in length). Note: The password is displayed as clear or encrypted text depending on whether or not 'password encryption' has been enabled on the AP. For more information on enabling password-encryption, see password-encryption on page 427 .
port <1025-65535>	Configures the port on which the MQTT Broker is reachable • <1025-65535> – Provide the port number form 1025 - 65535. Note: The default value is 61613.
server [<IP>|<HOST-NAME>]	Identifies the MQTT server either by its IP address or hostname. This the server hosting the MQTT Broker. • <IP> – Provide the server's IP address in the A.B.C.D format. • <HOST-NAME> – Provide the server's hostname. Note: The input should not exceed 255 characters in length.

topic-publish-prefix <LINE>	Configures the prefix of the topic published by the FMN • <LINE> – Specify the publish topic prefix. Note: The input should not exceed 255 characters in length.
topic-subscribe-prefix <LINE>	Configures the prefix of the topic subscribed by the FMN • <LINE> – Specify the subscribe topic prefix. Note: The input should not exceed 255 characters in length.
username <WORD>	Configures the username required to authenticate with the MQTT Broker. You will need a username/password combination in order for the FMN to authenticate and associate with the MQTT Broker. Use the 'username' and 'password' options to specify the username and password respectively. Note: The username should not exceed 32 characters in length.

```
tron reconstruct-nodetype-db-on-start
```

tron reconstruct-nodetype-db-on-start	Enables reconstruction of the node-type database. When enabled, the TRON software (FMN) discards existing database and on-the-fly, reconstructs a database containing "node-type" to a specific layout of GATT services and characteristics mappings. Each ID Node, within a physical space, sends out Bluetooth advertisements that includes the 'node-type' (for example, 0x11) information. When the TRON functionality on the WiNG AP, connects to an ID Node for the first time, it discovers and caches the ID Node's layout for GATT services and characteristics in the 'node-type' database/table. Subsequent GATT discovery of other ID Nodes is skipped on the assumption that ID Nodes advertising the same node-type value as the first ID Node will have the same layout for their GATT services and characteristics. This node-type database, created at the first instance of connection, persists across AP reboots and enabling/disabling of the TRON functionality on the AP. If on the ID Nodes, the layout of the GATT services and characteristics changes (post database creation), the existing database is no longer valid. In this scenario, use this command to discard the existing database and recreate a new one. Note: This parameter is not mandatory, and is disabled by default.

Examples

```
NOC-NX9500(config-profile-test8533-if-bluetooth1)#tron initial-config mqtt client-prefix fmn
NOC-NX9500(config-profile-test8533-if-bluetooth1)#tron initial-config mqtt server 1.2.3.4
NOC-NX9500(config-profile-test8533-if-bluetooth1)#tron initial-config mqtt topic-publish-prefix idnodes
NOC-NX9500(config-profile-test8533-if-bluetooth1)#tron initial-config mqtt topic-subscribe-prefix idnodes
NOC-NX9500(config-profile-test8533-if-bluetooth1)#tron initial-config mqtt username fmn
NOC-NX9500(config-profile-test8533-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  mode tron-tracking
  tron initial-config mqtt server 1.2.3.4
  tron initial-config mqtt username fmn
  tron initial-config mqtt password 0 fmn@1234
  tron initial-config mqtt client-prefix fmn
  tron initial-config mqtt topic-publish-prefix idnodes
  tron initial-config mqtt topic-subscribe-prefix idnodes
NOC-NX9500(config-profile-test8533-if-bluetooth1)#
```

Related Commands

no (bluetooth-inf-config-command) on page 1166	Removes the TRON related configurations set on this Bluetooth radio.

no (bluetooth-inf-config-command)

interface-config-bluetooth-instance on page 1152

Removes or reverts to default this Bluetooth radio interface's settings

Supported in the following platforms:

- Access Points – AP505i, AP510i/e, AP560i/h, AP7602, AP7612, AP7632, AP7662, AP8432, AP8533

Syntax

```
no [beacon|description|eddystone|ibeacon|mode|shutdown|tron]

no beacon [pattern|period]
no description
no eddystone [calibration-rssi|url [1|2]
no ibeacon [calibration-rssi|major|minor|uuid]
no mode
no shutdown
no tron [ignore-mqtt-truststore|initial-config|reconstruct-nodetype-db-on-start]
no tron [ignore-mqtt-truststore|reconstruct-nodetype-db-on-start]
no tron initial-config mqtt [client-prefix|password|port|server|topic-publish-prefix|topic-subscribe-prefix|username]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes or reverts to default this Bluetooth radio interface's settings based on the parameters passed • <PARAMETERS> – Specify the parameters.

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 853

The following table summarizes NAT pool configuration commands:

Command	Description
ip on page 1167	Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards, etc.
nat-pool-config-instance on page 1173	Invokes NAT pool configuration parameters

ip

ip on page 1167

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]]
```

ip	Configures IPv4 routing components
default-gateway	Configures default gateway (next-hop router) parameters
<IP>	Configures default gateway's IP address • <IP> – Specify the default gateway's IP address.
failover	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.
<HOST-ALIAS-NAME>	Configures the host alias mapped to the required default gateway • <HOST-ALIAS-NAME> – Specify the host alias name (should be existing and configured). Host alias names begin with a '$'.
priority [dhcp-client <1-1800>| static-route <1-1800>]	Configures default gateway priority • dhcp-client <1-1800> – Defines a priority for the default gateway acquired by the DHCP client on the VLAN interface. The default setting is 1000. • static-route <1-1800> – Defines the weight (priority) assigned to this static route versus others that have been defined to avoid potential congestion. The default setting is 100. The following keyword is common to 'dhcp-client' and 'static-route' parameters: • <1-1800> – Specify the priority from 1 - 18000 (lower the value higher is the priority).

```
ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]
```

ip	Configures IPv4 routing components
dns-server-forward	Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This option is disabled by default.
domain-lookup	Enables domain lookup. When enabled, human friendly domain names are converted into numerical IP destination addresses. The option is enabled by default.
domain-name <DOMAIN-NAME>	Configures a default domain name • <DOMAIN-NAME> – Specify a name for the DNS (should not exceed 64 characters in length).
name-server <IP>	Configures the name server's IP address • <IP> – Specify the IP address of the name server.
routing	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]
```

ip	Configures IPv4 routing components
dhcp	Configures the DHCP client and host
client [hostname| persistent-lease]	Sets the DHCP client • hostname – Includes the hostname in the DHCP lease for the requesting client. This option is enabled by default. • 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.

```
ip igmp snooping {fast-leave|forward-unknown-multicast}
```

ip	Configures IPv4 routing components
fats-leave	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. This feature is supported only on the AP7502, AP8533 model access points.
igmp snooping forward-unknown-multicast	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>}
```

ip	Configures IPv4 routing components
igmp snooping querier	Optional. Enables the IGMP querier functionality for the specified VLAN. By default IGMP snooping querier is disabled.
max-response-time <1-25>	Configures the IGMP maximum query response interval used in IGMP V2/V3 queries for the given VLAN. The default is 10 seconds.
query-interval <1-18000>	Configures the IGMP querier query interval in seconds. Specify a value from 1 - 18000 seconds. The default is 60 seconds.
robustness-variable <1-7>	Configures the IGMP robustness variable from 1 - 7. The default is 2.
timer expiry <60-300>	Configures the other querier time out value for the given VLAN. The default is 60 seconds.
version <1-3>	Configures the IGMP query version for the given VLAN. The default is 3.

```
ip nat [crypto source pool|pool <NAT-POOL-NAME>]
```

ip	Configures IPv4 routing components
nat	Configures the NAT parameters

crypto source pool <NAT-POOL-NAME>	Configures the NAT source address translation settings for IPSec tunnels • <NAT-POOL-NAME> – Specify a NAT pool name.
pool <NAT-POOL-NAME>	Configures a pool of IP addresses for NAT • <NAT-POOL-NAME> – Specify a name for the NAT pool.

```
ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp]
[(<NATTED-IP> {<1-65535>})]
```

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the destination • inside – Configures inside address translation • outside – Configures outside address translation
destination static <ACTUAL-IP>	The following keywords are common to the 'inside' and 'outside' parameters: • destination – Specifies destination address translation parameters • static – Specifies static NAT local to global mapping <ACTUAL-IP> – Specify the actual outside IP address to map.
<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures Transmission Control Protocol (TCP) port • udp – Configures User Datagram Protocol (UDP) port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

```
ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp]
[(<NATTED-IP> {<1-65535>})]
```

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the source • inside – Configures inside address translation • outside – Configures outside address translation
source static <ACTUAL-IP>	The following keywords are common to the' inside' and 'outside' parameters: • source – Specifies source address translation parameters • static – Specifies static NAT local to global mapping <ACTUAL-IP> – Specify the actual inside IP address to map.

<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures the TCP port • udp – Configures the UDP port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 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	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside IP access list
source list <IP-ACCESS-LIST-NAME>	Configures an access list describing local addresses • <IP-ACCESS-LIST-NAME> – Specify a name for the IP access list.
interface [<INTERFACE-NAME>| pppoe1| vlan <1-4094>| wwan1]	Selects an interface to configure. Select a layer 3 router interface or a VLAN interface. • <INTERFACE-NAME> – Selects a layer 3 interface. Specify the layer 3 router interface name. • vlan – Selects a VLAN interface • <1-4094> – Set the SVI VLAN ID of the interface. • pppoe1 – Selects PPP over Ethernet interface • wwan1 – Selects Wireless WAN interface
address <IP>	The following keyword is recursive and common to all interface types: • address <IP> – Configures the interface IP address used with NAT
interface <L3-IF-NAME>	The following keyword is recursive and common to all interface types: • interface <L3-IF-NAME> – Configures a wireless controller or service platform's VLAN interface • <L3IFNAME> – Specify the SVI VLAN ID of the interface.
overload	The following keyword is recursive and common to all interface types: • overload – Enables use of global address for many local addresses
pool <NAT-POOL-NAME>	The following keyword is recursive and common to all interface types: • pool <NAT-POOL-NAME> – Specifies the NAT pool • <NAT-POOL-NAME> – Specify the NAT pool name.

```
ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]
```

ip	Configures IPv4 routing components
route	Configures the static routes
<IP/M>	Specify the IP destination prefix in the A.B.C.D/M format.

<IP>	Specify the IP address of the gateway.
<HOST-ALIAS-NAME>	Configures the host alias mapped to the required default gateway • <HOST-ALIAS-NAME> – Specify the host alias name (should be existing and configured). Host alias names begin with a '$'.

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

no on page 1214	Disables or reverts settings to their default

nat-pool-config-instance

ip on page 1167

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
address on page 1174	Configures NAT pool addresses
no on page 1175	Negates a command or sets its default

address

nat-pool-config-instance on page 1173

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
address [<IP>|range <START-IP> <END-IP>]
```

Parameters

```
address [<IP>|range <START-IP> <END-IP>]
```

address <IP>	Adds a single IP address to the NAT pool
range <START-IP> <END-IP>	Adds a range of IP addresses to the NAT pool • <START-IP> – Specify the starting IP address of the range. • <END-IP> – Specify the ending IP address of the range.

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

no on page 1214	Removes address(es) configured with this NAT pool

no

nat-pool-config-instance on page 1173

Removes address(es) configured with this NAT pool

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no address [<IP>|range <START-IP> <END-IP>]
```

Parameters

```
no address [<IP>|range <START-IP> <END-IP>]
```

no address [<IP>| range <START-IP> <END-IP>]	Removes a single IP address or a range of IP addresses from this NAT pool

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)#
```

ipv6

Profile Config Commands on page 853

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.

Note
The IPv6 settings configured at the profile/device level are global configuration settings and not interface-specific.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]
```

ipv6	Configures IPv6 routing components
default-gateway <IPv6> {vlan <VLAN-ID>}	Configures IPv6 default gateway's address in the ::/0 format • vlan <VLAN-ID> – Optional. Specify the VLAN interface's ID through which the default gateway is accessible.
dns-server-forward	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.
hop-limit <1-255>	Configures the IPv6 hop count limit • <1-255> – Specify a value between 1 - 255. The default is 64.
name-server <IPv6>	Configures the IPv6 name server's address • <IPv6> – Specify the address of the IPv6 name server.
nd-reachable-time <5000-3600000>	Configures the time, in milliseconds, that a neighbor is assumed to be reachable after having received neighbor discovery (ND) confirmation for their reachability • <5000-3600000> – Specify a value from 5000 - 3600000 milliseconds. The default is 30,000 milliseconds.

ns-interval <1000-3600000>	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. • <1000-3600000> – Specify a value from 1000 - 3600000. The default is 1000 milliseconds.
ula-reject-route	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.
unicast-routing	Enables IPv6 unicast routing. This feature is enabled by default.

```
ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}
```

ipv6	Configures IPv6 routing components
ra-convert {throttle interval <3-1800> max-RAs <1-256>	Enables conversion of multicast router advertisements (RAs) to unicast RAs at the dot11 layer. This feature is disabled by default. • throttle – Optional. Throttles multicast RAs before converting to unicast • interval <3-1800> – Throttles multicast RAs for a specified time period. Specify the interval from 3 - 1800 seconds. The default is 3 seconds. max-RAs <1-256> – Specifies the maximum number of RAs per IPv6 router during the specified throttle interval. Specify a value from 1 - 256. The default is 1.

```
ipv6 mld snooping {forward-unknown-multicast}
```

ipv6	Configures IPv6 routing components
mld snooping forward-unknown-multicast	Enables multicast listener discovery (MLD) protocol snooping. This feature is disabled by default. 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. • forward-unknown-multicast – Optional. Enables unknown multicast forwarding. This feature is enabled by default.

```
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	Configures IPv6 routing components
mld snooping querier	Enables MLD protocol snooping • 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.
max-response-time <1-25000>	`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. • <1-25000> – Specify a value from 1 - 25000 milliseconds. The default is 10 milliseconds.
query-interval <1-18000>	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. • <1-18000> – Specify a value from 1 - 18000 seconds. The default is 60 seconds.
robustness-variable <1-7>	Configures the MLD IGMP robustness variable. This value is used by the sender of a query. • <1-7> – Select a value from 1 - 7. The default is 2.
timer expiry <60-300>	Configures the MLD other querier (any external querier) timeout • <60-300> – Specify a value from 60 - 300 seconds. The default is 60 seconds.
version <1-2>	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. • <1-2> – Select the MLD version from 1 - 2. The default is 2.

```
ipv6 neighbor <IPv6> <MAC> [<INTF-NAME>|pppoe1|vlan <1-4094>|wwan1] {dhcp-server|router}
```

ipv6	Configures IPv6 routing components
neighbor	Configures static IPv6 neighbor entries
<IPv6>	Specify the IPv6 address for which a static neighbor entry is created.
<MAC>	Specify the MAC address associated with the specified IPv6 address.

[<INTF-NAME>| pppoe1| vlan <1-4094>| wwan1]	Specify the following interface settings: • <INTF-NAME> – Selects the layer 3 router interface. Specify the interface name. • pppoe1 – Selects the PPP over Ethernet interface • vlan <1-4094> – Selects the VLAN interface. Specify the VLAN interface index. • wwan1 – Selects the wireless WAN interface
{dhcp-server|router}	After specifying interface type, you can optionally specify the device type for this neighbor solicitation. • dhcp-server – Optional. States this neighbor entry is for a DHCP server • router – Optional. States this neighbor entry is for a router

```
ipv6 neighbor timeout <15-86400>
```

neighbor	Configures static IPv6 neighbor entries
timeout <15-86400>	Configures the timeout, in seconds, for the static neighbor entries • <15-86400> – Specify a value from 15 - 86400 seconds. The default is 3600 seconds.

```
ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID>}
```

ipv6	Configures IPv6 routing components
route	Configures the static routes These routes are maintained in the IPv6 Forwarding Information Base (FIB). To view FIB6 routing entries, use the service > show fib6 > <TABLE-ID> command.
<DEST-IPv6-PREFIX/PREFIX-LENGTH>	Specify the IPv6 destination prefix (IPV6 network) and the prefix length.
<IPv6-GATEWAY-ADDRESS>	Specify the IPv6 gateway's address.
vlan <VLAN-ID>	Optional. specify the VLAN interface's ID (through which the defalut gateway is accessible) This parameter is needed only if the gateway address is a link local address.

Example

```
nx9500-6C8809(config-profile-TestRFS4000)#ipv6 default-gateway 2001:10:10:10:10:10:10:2

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 2001:10:10:10:10:10:10:2
 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

no on page 1214	Disables or reverts IPv6 settings to their default

l2tpv3

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]
```

l2tpv3	Configures the L2TPv3 protocol settings for a profile
hostname <HOSTNAME>	Configures the host name sent in the L2TPv3 signaling 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. • <HOSTNAME> – Specify the L2TPv3 specific host name.
inter-tunnel-bridging	Enables inter tunnel bridging of packets. This feature is disabled by default.
manual-session	Creates/modifies L2TPv3 manual sessions For more information, see l2tpv3-manual-session-commands on page 1724.

router-id [<1-4294967295>| <IP>]	Configures the router ID (either the numeric IP address or the integer) sent in the L2TPv3 signaling messages. These signaling (AVP) messages help to identify tunneled peers. • <1-4294967295> – Configures the router ID in decimal format from 1 - 4294967295 • <IP> – Configures the router ID in the IP address (A.B.C.D) format
tunnel	Creates/modifies an L2TPv3 tunnel For more information, see l2tpv3-tunnel-commands on page 1710.
udp-listen-port <1024-65535>	Configures the UDP port used to listen for incoming traffic • <1024-65535> – Specify the UDP port from 1024 - 65535 (default is 1701)

```
l2tpv3 logging ip-address [<IP>|any] hostname [<HOSTNAME>|any] router-id [<IP>|<WORD>|any]
```

l2tpv3	Configures L2TPv3 protocol settings for a profile
logging	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.
ip-address [<IP>|any]	Configures the L2TPv3 peer tunnel IP address for which event logging is enabled. The options are: • <IP> – Specify the peer's IP address. L2TPv3 events are captured and logged for the specified peer. • any – Peer's IP address is not specified. Enables event logging for all incoming connections from any IP address.
hostname [<HOSTNAME>| any]	Configures the L2TPv3 peer tunnel hostname for which event logging is enabled. The options are: • <HOSTNAME> – Specify the peer's host name. L2TPv3 events are captured and logged for specified host. • any – Peer's hostname is not specified. Enables debugging for all incoming connections from any host.
router-id [<IP>|<WORD>|any]	Configures the L2TPv3 tunnel router ID for which event logging is enabled. The options are: • <IP> – Specify the router ID in the IP address format. • <WORD> – Specify the router ID in the form of an integer or range. For example 100-200. • any – Router ID is not specified. Enables debugging for all incoming connections from any L2TPv3 router.

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

no on page 1214	Negates a L2TPv3 tunnel settings on this profile

l3e-lite-table

Profile Config Commands on page 853

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 — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`l3e-lite-table aging-time <10-1000000>`

Parameters

```
l3e-lite-table aging-time <10-1000000>
```

l3e-lite-table aging-time <10-1000000>	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.

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

no on page 1214	Removes the L3e lite table aging time configuration

led

Profile Config Commands on page 853

Turns on and off access point LEDs

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`led {flash-pattern}`

Parameters

```
led {flash-pattern}
```

led flash-pattern	Optional. Enables LED flashing on the device using this profile 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

no on page 1214	Disables or reverts settings to their default

led-timeout

Profile Config Commands on page 853

Configures the LED-timeout timer in the device or profile configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1214	Disables LED-timeout timer

legacy-auto-downgrade

Profile Config Commands on page 853

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
legacy-auto-downgrade
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-default-rfs4000)#legacy-auto-downgrade
```

Related Commands

no on page 1214	Prevents device firmware from auto downgrading when legacy devices are detected

legacy-auto-update

Profile Config Commands on page 853

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>
```

legacy-auto-update	Updates a legacy AP7161 access point firmware
ap71xx image <FILE>	Auto updates legacy AP7161 firmware • image – Sets the path to the firmware image • <FILE> – Specify the path and filename in the flash:/ap.img format.

Example

```
nx9500-6C8809(config-profile-default-rfs4000)#legacy-auto-update ap71xx image flash:/
ap47d.img
```

Related Commands

no on page 1214	Disables automatic legacy firmware upgrade

lldp

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

lldp	Enables LLDP on this profile and configures LLDP settings
holdtime <10-1800>	Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding. • <10-1800> – Specify a holdtime from 10 - 1800 seconds. The default is 180 seconds.

run	Enables LLDP on this profile
timer <5-900>	Sets the transmit interval. This command specifies the transmission frequency of LLDP updates in seconds. • <5-900> – Specify transmit interval from 5 - 900 seconds. The default is 60 seconds.

```
lldp med-tlv-select [inventory-management|power-management {auto}]
```

lldp	Enables LLDP on this profile and configures LLDP settings
med-tlv-select [inventory-management| power-management {auto}]	Provides additional media endpoint device TLVs to enable inventory and power management discovery. Specifies the LLDP MED TLVs to send or receive. • 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. • 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. • auto – Optional. Assigns default value based on device type

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

no on page 1214	Disables LLDP on this profile

load-balancing

Profile Config Commands on page 853

Configures load balancing parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

load-balancing advanced-params	Configures advanced load balancing parameters
2.4GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 2.4 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 2.4 GHz load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.
5GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 5.0 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.
ap-load [client-weightage| throughput-weightage] <0-100>	Configures AP load calculation weightages • client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.

```
load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>
```

load-balancing advanced-params	Configures advanced load balancing parameters
equality-margin [2.4GHz|5GHz|ap|band] <0-100>	Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, APs, or bands. • 2.4GHz – Configures the maximum load difference considered equal when comparing loads on different 2.4 GHz channels • 5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels • ap – Configures the maximum load difference considered equal when comparing loads on different APs • band – Configures the maximum load difference considered equal when comparing loads on different bands The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands: • <0-100> – 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%.

```
load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz] <0-100>
```

load-balancing advanced-params	Configures advanced load balancing parameters
hiwater-threshold	Configures the load beyond which load balancing is invoked
[ap|channel-2.4GHz| channel-5GHz] <0-100>	Select one of the following options: • ap – Configures the AP load beyond which load balancing begins • channel-2.4GHz – Configures the AP load beyond which load balancing begins (for APs on 2.4 GHz channel) • channel-5GHz – Configures the AP load beyond which load balancing begins for (APs on 5.0 GHz channel) The following keyword is common for the 'AP', 'channel-2.4GHz', and 'channel-5GHz' parameters: • <0-100> – 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.

```
load-balancing advanced-params max-preferred-band-load [2.4GHGz|5GHzd] <0-100>
```

load-balancing advanced-params	Configures advanced load balancing parameters
max-preferred-band-load	Configures the maximum load on the preferred band, beyond which the other band is equally preferred
[2.4GHz|5GHz] <0-100>	Select one of the following options: • 2.4GHz – Configures the maximum load on 2.4 GHz, when it is the preferred band • 5GHz – Configures the maximum load on 5.0 GHz, when it is the preferred band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <0-100> – Configures the maximum load as a percentage from 0 - 100. The default value for 2.4GHz and 5.GHz is 75%.

```
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 advanced-params	Configures advanced load balancing parameters
max-neighbors <0-16>	Configures the maximum number of confirmed neighbors to balance • <0-16> – Specify a value from 0 - 16. Optionally configure a minimum of 0 neighbors and a maximum of 16 neighbors. The default is 16.
min-common-clients <0-256>	Configures the minimum number of common clients that can be shared with the neighbor for load balancing • <0-256> – Specify a value from 0 - 256. Optionally configure a minimum of 0 clients and a maximum of 256 clients. The default is 0.
min-neighbor-rssi <-100-30>	Configures the minimum signal strength (RSSI) of a neighbor detected • <-100-30> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -65 dBm.
min-probe-rssi <-100-30>	Configures the minimum received probe signal strength required to qualify the sender as a common client • <0-100> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -100 dBm.

```
load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]
```

load-balancing	Configures the following load balancing parameters: ap-loads, band-loads, and channel-loads.
balance-ap-loads	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.
balance-band-loads	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.
balance-channel-loads [2.4GHz| 5GHz]	Enables the following: • 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. • 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.

```
load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz| prefer-5GHz]
```

load-balancing band-control-strategy	Configures a band control strategy 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.
distribute-by-ratio	Distributes clients to either band according to the band-ratio
prefer-2.4GHz	Nudges all dual-band clients to 2.4 GHz band
prefer-5GHz	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>]
```

load-balancing band-ratio	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.
2.4GHz [0|<1-10>]	Configures the relative loading of 2.4 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 0.
5ghz [0|<1-10>]	Configures the relative loading of 5.0 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 1.

```
load-balancing group-id <GROUP-ID>
```

load-balancing group-id <GROUP-ID>	Configures group ID to facilitate load balancing • <GROUP-ID> – Specify the group ID. This option is enabled only when a group ID is configured.

```
load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification|
use-smart-rf]
```

load-balancing neighbor-selection-strategy	Configures a neighbor selection strategy. The options are: use-common-clients, use-roam-notification, and use-smart-rf
use-common-clients	Selects neighbors based on probes from clients common to neighbors. This option is enabled by default.
use-roam-notification	Selects neighbors based on roam notifications from roamed clients. This option is enabled by default.
use-smart-rf	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

no on page 1214	Disables load balancing on this profile

logging

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

logging	Enables message logging and configures logging settings
aggregation-time <1-60>	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. • <1-60> – Specify a value from 1 - 60 seconds. The default value is 0.
host [<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. • <IPv4> – Specify the IPv4 address of the remote host. • <IPv6> – Specify the IPv6 address of the remote host. • port <1-65535> – Optional. Configures the syslog port <1-65535> – Specify the syslog port from 1 - 65535. The default port is 514.
on	Enables the logging of system messages

```
logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|
errors|warnings|notifications|informational|debugging]
```

logging	Enables message logging and configures logging settings
buffered	Sets the buffered logging level
console	Sets the console logging level
syslog	Sets the syslog server's logging level
forward	Forwards system debug messages to the wireless controller or service platform
[<0-7>|alerts| criticail|debugging| emergencies|errors| informational| notifications| warnings]	The following keywords are common to the buffered, console, syslog, and forward parameters. All incoming messages have different severity levels based on their importance. The severity level is fixed on a scale of 0 - 7. • <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 (default) • notifications – Severity level 5: Normal but significant conditions • informational – Severity level 6: Informational messages • debugging – Severity level 7: Debugging messages

```
logging facility [local0|local1|local2|local3|local4|local5|local6|local7]
```

logging	Enables message logging and configures logging settings
facility [local0|local1| local2|local3| local4| local5|local6|local7]	Enables the syslog to decide where to send the incoming message There are 8 logging facilities, from syslog0 to syslog7. • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7

Example

```
NOC-NX9500(config-profile-testNX9000)#logging facility local4

NOC-NX9500(config-profile-testNX9000)#show context include-factory | include log
ging
 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

no on page 1214	Disables logging on this profile

mac-address-table

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

mac-address-table aging-time [0|<10-1000000>]	Sets the duration a learned MAC address persists after the last update • 0 – Entering the value '0' disables the aging time • <10-1000000> – Sets the aging time from 10 -100000 seconds. The default is 300 seconds.

```
mac-address-table detect-gateways
```

mac-address-table detect-gateways	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>]
```

mac-address-table static <MAC>	Creates a static MAC address table entry • <MAC> – 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.
vlan <1-4094>	Assigns a static MAC address to a specified VLAN port • <1-4094> – Specify the VLAN index from 1 - 4094.

interface [<L2-INTERFACE>| ge <1-4>| port-channel <1-2>]	Specifies the interface type. The options are: layer 2 Interface, GigabitEthernet interface, and a port channel interface
	• <L2-INTERFACE> – Specify the layer 2 interface name.
	• ge – Specifies a GigabitEthernet interface
	  • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
	• port-channel – Specifies a port channel interface
	  • <1-2> – Specify the port channel interface index from 1 - 2.

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

no on page 1214	Disables or reverts settings to their default

mac-auth

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`mac-auth use aaa-policy <AAA-POLICY-NAME>`

Parameters

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

mac-auth	Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.
use aaa-policy <AAA-POLICY-NAME>	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

no on page 1214	Disables authentication of MAC addresses on wired ports settings on this profile (or device)

management-server

Profile Config Commands on page 853

Configures a management server with this profile. This command is also applicable to the device configuration context.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 ExtremeCloud Appliance controller's IP address or hostname as the management server. For information on configuring the adoption-mode, see adoption-mode on page 858.

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

no on page 1214	Removes the management server configuration

meshpoint-device

Profile Config Commands on page 853

Configures meshpoint device parameters. This feature is configurable in the profile and device configuration modes.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 1811.

```
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

no on page 1214	Removes a specified meshpoint

Note

For more information on the meshpoint-device configuration parameters, see Meshpoint Policy on page 1773.

meshpoint-monitor-interval

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
meshpoint-monitor-interval <1-65535>
```

Parameters

```
meshpoint-monitor-interval <1-65535>
```

meshpoint-monitor-interval <1-65535>	Configures the meshpoint monitoring interval in seconds • <1-65535> – Specify the interval from 1 - 65535 seconds. The default is 30 seconds.

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

no on page 1214	Resets the meshpoint monitoring interval to default (30 seconds)

min-misconfiguration-recovery-time

Profile Config Commands on page 853

Configures the minimum device connectivity verification time

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
min-misconfiguration-recovery-time <60-3600>
```

Parameters

```
min-misconfiguration-recovery-time <60-3600>
```

min-misconfiguration-recovery-time <60-3600>	Configures the minimum connectivity (with the associated device) verification interval • <60-3600> – Specify a value from 60 - 3600 seconds (default is 60 seconds).

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

no on page 1214	Resets setting to default (60 seconds)

mint

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
dis priority-adjustment <-255-255>	Sets the relative priority for the router to become DIS (designated router) • priority-adjustment – Sets priority adjustment added to base priority 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. • <-255-255> – Specify a value from -255 - 255. The default is 0. Higher numbers result in higher priorities
strict-evis-reachability	Enables reaching EVI *(Ethernet Virtualization Interconnect)* election winners through MiNT. This option is enabled by default.

```
mint inter-tunnel-bridging
```

mint	Configures MiNT protocol parameters required for MiNT link creation, adoption and communication
inter-tunnel-bridging	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>]
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
level 1	Configures local MiNT routing settings • 1 – Configures local MiNT routing level
area-id [<1-16777215>| <NUMBER-ALIAS-NAME>]	Specifies the level 1 routing area identifier. Use one of the following options to specify the area ID: • <1-16777215> – Specify a value from 1 - 16777215. • <NUMBER-ALIAS-NAME> – 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 alias on page 172.

```
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>]}}
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
link force	Creates a MiNT routing link as a forced link • force – Forces a MiNT routing link to be created even if not necessary
ip [<IPv4>|<IPv6>]	Creates a MiNT tunnel over UDP/IPv4 or IPv6 Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MINT protocol. • <IPv4> – Specify the MiNT tunnel peer's IPv4 address. • <IPv6> – Specify the MiNT tunnel peer's IPv6 address. 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.
<1-65535> level 2	Optional. Specifies a custom UDP port for MiNT links. Specify the port from 1 - 65535. • level – Specifies the routing level • 2 – Configures level 2 inter-site MiNT routing
adjacency-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100.

hello-interval <1-120>	Optional. Specifies the interval, in seconds, between successive hello packets • <1-120> – Specify a value from 1 - 120 seconds. The default is 15 seconds.
ipsec-security {gw [<IP>|<HOST-NAME>]}	Optional. Enables IPSec secure peer authentication on the MiNT link connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – 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.

```
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>]}}
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
link listen ip [<IPv4>|<IPv6>| <HOST-ALIAS-NAME>]	Creates a MiNT routing link • listen – Creates a MiNT listening link • ip – Creates a MiNT listening link over UDP/IP or IPv6 <IPv4> – Specify the IPv4 address of the listening UDP/IP link. <IPv6> – Specify the IPv6 address of the listening UDP/IP link. <HOST-ALIAS-NAME> – Specify the host alias identifying the MiNT link address. The host alias should existing and configured. 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.
link vlan <1-4094>	Enables MiNT routing on VLAN • vlan – Defines a VLAN ID used by peers for inter-operation when supporting the MINT protocol. • <1-4094> – Select VLAN ID from 1 - 4094.
adjacency-hold-time <2-600>	This parameter is common to the 'listen' and 'vlan' parameters: • adjacency-hold-time <2-600> – Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds. For MiNT VLAN routing, the default is 13 seconds.
cost <1-100000>	This parameter is common to the 'listen' and 'vlan' parameters: • cost <1-100000> – Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100. For MiNT VLAN routing, the default is 10.

hello-interval <1-120>	This parameter is common to the 'listen' and 'vlan' parameters: • hello-interval <1-120> – Optional. Specifies the interval, in seconds, between successive hello packets • <1-120> – Specify a value from 1 - 120. The default is 15 seconds. For MiNT VLAN routing the default is 4 seconds.
level [1|2]	This parameter is common to the 'listen' and 'vlan' parameters: Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw [<IP>| <HOST-NAME>]}	This parameter is common to the 'listen' and 'vlan' parameters: • ipsec-security – Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – 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.

```
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>]}}
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
link ip [<IPv4>|<IPv6>| <HOST-ALIAS-NAME>]	Creates a MiNT routing link • ip – Creates a MiNT tunnel over UDP/IP or IPv6 Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MINT protocol. • <IPv4> – Specify the IPv4 address used by peers. • <IPv6> – Specify the IPv6 address used by peers. • <HOST-ALIAS-NAME> – Specify the host alias identifying the MiNT tunnel peer's address. The host alias should existing and configured.
<1-65535>	Select the peer UDP port from 1 - 65535.
adjacency-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100.
hello-interval <1-120>	Optional. Specifies the interval, in seconds, between successive hello packets • <1-120> – Specify a value from 1 - 120. The default is 15 seconds.

level [1|2]	Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw [<IP>| <HOST-NAME>]}	Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – 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.

```
mint mlcp [ip|ipv6|vlan]
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
mlcp [ip|ipv6|vlan]	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. • vlan – Enables MLCP over layer 2 (VLAN) links • ip – Enables MLCP over layer 3 (UDP/IP) links. When enabled, allows adoption over IPv4 address. • ipv6 – Enables MLCP over layer 3 (UDP/IPv6) links. When enabled, allows adoption over IPv6 address.

```
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	Configures MiNT protocol parameters required for MiNT link creation and adoption
mint rate-limit level2	Applies rate limits on extended VLAN traffic 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. 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).

link [ip <IPv4/IPv6> <1-65535>| vlan <1-4094>]	Configures rate limit parameters applicable for all statically configured MiNT links on level2. Select the link-type as 'IP' or 'VLAN'. • ip <IPv4/IPv6> – Configures rate limits for MiNT link traffic over UDP/IP • <IPv4/IPv6> – Specify the MiNT peer's IPv4 or IPV6 address in the A.B.C.D and X:X::X:X formats respectively. <1-65535> – Configures the virtual port used for rate limiting traffic. Specify the UDP port from 1 - 65535. • vlan <1-4094 – Configures rate limits for MiNT link traffic on specified VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094.
mlcp [ip|ipv6|vlan]	Configures rate limit parameters applicable for MLCP 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. • ip – Configures rate-limits for MLCP over UDP/IPv4 links • ipv6 – Configures rate-limits for MLCP over UDP/IPv6 links • vlan – Configures rate-limits for MLCP over VLAN links
rate <50-1000000>	Configures the rate limit from 50 - 1000000 Kbps 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.

max-burst-size <2-1024>	Configures the maximum burst size from 0 - 1024 Kbytes 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.
red-threshold [background|best-effort|video|voice] <0-100>	Optional. Configures the RED *(random early detection)* threshold (as a percentage) for the following traffic types: • 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%. • 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%. • 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%. • 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%. • <0-100> – After selecting the traffic type, specify the RED threshold from 0 - 100%.

```
mint spf-latency <0-60>
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
spf-latency <0-60>	Specifies the latency of SPF routing recalculation 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. • <0-60> – Specify the latency from 0 - 60 seconds.

```
mint tunnel-across-extended-vlan
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
tunnel-across-extended-vlan	Enables tunneling of MiNT protocol packets across an extended VLAN. This setting is disabled by default.

```
mint tunnel-controller-load-balancing level1
```

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
tunnel-controller-load-balancing level1	Enables load balancing of MiNT extended VLAN traffic across tunnels • level1 – Enables balancing of load of a tunnel wireless controller or service platform over VLAN links

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

no on page 1214	Disables or reverts settings to their default

misconfiguration-recovery-time

Profile Config Commands on page 853

Verifies connectivity after a configuration is received

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
misconfiguration-recovery-time [0|<60-300>]
```

Parameters

```
misconfiguration-recovery-time [0|<60-300>]
```

<60-300>	Sets the recovery time from 60 - 300 seconds (default is 180 seconds)
0	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

no on page 1214	Reverts to default (180 seconds)

neighbor-inactivity-timeout

Profile Config Commands on page 853

Configures neighbor inactivity timeout

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
neighbor-inactivity-timeout <1-1000>
```

Parameters

```
neighbor-inactivity-timeout <1-1000>
```

<1-1000>	Sets neighbor inactivity timeout • <1-1000> – Specify a value from 1 - 1000 seconds. The default is 30 seconds.

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 me1
 interface ge1
  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 853

Configures the neighbor information exchange interval

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`neighbor-info-interval <1-100>`

Parameters

```
neighbor-info-interval <1-100>
```

<1-100>	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 853

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

no <PARAMETERS>	Removes or reverts this profile'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-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 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`noc update-interval [<5-3600>|auto]`

Parameters

```
noc update-interval [<5-3600>|auto]
```

noc update-interval [<5-3600>| auto]	Configures NOC statistics update interval • <5-3600> – Specify the update interval from 5 - 3600 seconds. • 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.

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

no on page 1214	Resets NOC related parameters

nsight

Profile Config Commands on page 853

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 1219.

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, 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]
```

nsight database statistics	Configures NSight database statistics related parameters
avc-update-interval	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. 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.

update-interval	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. 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. Note: Use the 'avc-update-interval' and 'wireless-clients-update-interval' keywords to configure update interval for AVC-related and wireless-clients related information respectively.
wireless-clients-update-interval	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. 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.
[120|30|300|60|600]	The following keywords are common to all of the above parameters: • 120 – Sets the data-update periodicity as 120 seconds (2 minutes) • 30 – Sets the data-update periodicity as 30 seconds • 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. • 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the 'update-interval' parameter. • 600 – Sets the data-update periodicity as 600 seconds (10 minutes)

```
nsight database statistics max-apps-per-client <1-1000>
```

nsight database statistics	Configures NSight database statistics related parameters
max-apps-per-client	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.
<1-1000>	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>
```

nsight database statistics	Configures NSight database statistics related parameters
[max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata| max-ssl-visits-metadata]	Configures the number of HTTP and/or SSL metadata posted within an update interval • max-http-usage-metadata – Configures the NSight database maximum http-metadata by usage (rx+tx) to be posted in an update-interval • max-http-visits-metadata – Configures the NSight database's maximum http-metadata by the number of visits to be posted within an update-interval • max-ssl-usage-metadata – Configures the NSight database maximum ssl-metadata by usage (rx+tx) to be posted in an update-interval • max-ssl-visits-metadata – Configures the NSight database's maximum ssl-metadata by the number of visits to be posted within an update-interval The following keyword is common to all of the above mentioned metadata options: • <1-1000> – Specify a value from 1 - 1000. The default is 10 metadata for each.

```
nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```

nsight database summary	Configures the NSight database's per-bucket data storage duration
duration <1-24> <1-168> <1-2160> <24-26280>	Configures the duration for which data is stored on a per-bucket basis • <1-24> – Specify the bucket 1 duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours. • <1-168> – Specify the bucket 2 duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours. <1-2160> – Specify the bucket 3 duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours). <24-26280> – Specify the bucket 4 duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year). 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 use (rf-domain-config-mode) on page 488,) 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.

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

no on page 1287	Reverts the NSight database related parameters configured to default values

ntp

Profile Config Commands on page 853

Configures the NTP *(Network Time Protocol)* 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>}
```

ntp server <PEER-IP/HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
autokey	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]}
```

ntp server <PEER-IP/HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
maxpoll [1024|2048|4096| 8192]	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: • 1024 – Configures the maximum polling interval as 1024 seconds. This is the default setting. • 2048 – Configures the maximum polling interval as 2048 seconds • 4096 – Configures the maximum polling interval as 4096 seconds • 8192 – Configures the maximum polling interval as 8192 seconds

```
ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}
```

ntp server <PEER-IP/HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
minpoll [1024|128|256|512| 64]	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: • 1024 – Configures the minimum polling interval as 1024 seconds • 128 – Configures the minimum polling interval as 128 seconds • 256 – Configures the minimum polling interval as 256 seconds • 512 – Configures the minimum polling interval as 512 seconds • 64 – Configures the minimum polling interval as 64 seconds. This is the default setting.

```
ntp server <PEER-IP/HOSTNAME> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}
```

ntp server <PEER-IP/HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME>> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
key <1-65534> md5 [0 <WORD>| 2 <WORD>|<WORD>]	Optional. Defines the authentication key for the specified NTP server. This option is used to configure the key when 'autokey' configuration is not enabled. • <1-65534> – Specify the peer key number. Should not exceed 64 characters in length. • md5 – Sets MD5 authentication 0 <WORD> – Configures a clear text password 2 <WORD> – Configures an encrypted password <WORD> – Sets an authentication key

```
ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}
```

ntp server <PEER-IP/HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
prefer version <1-4>	Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. • version – Optional. Configures the NTP version • <1-4> – 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.
version <1-4> prefer	Optional. Configures the version number used by the specified NTP server resource • <1-4> – 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. • 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 <1-4>' keyword is applied to this preferred NTP resource.

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 1214	Disables or reverts settings to their default

otls

Profile Config Commands on page 853

Enables support for OTLS *(OmniTrail Location Server)* 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 — AP510

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>
```

otls apid <WORD>	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. • <WORD> – Specify an ID for the AP. 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>
```

otls control-port <0-65535>	Configures the port used by the AP to establish and maintain connection with the OTLS server • <0-65535> – Specify the control port from 0 - 655635.

```
otls data-port [2.4GHz|5GHz] <0-65535>
```

otls data-port [2.4GHz|5GHz] <0-65535>	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 otls > forward > [2.4GHz|5GHz] > [disable|enable] command to enable data forwarding. • 2.4GHz – Configures the port used to forward OTLS beacons received on the 2.4 GHz band • 5.0GHz – Configures the port used to forward OTLS beacons received on the 5.0 GHz band The following keyword is common to the above parameters: • <0-65535> – Specify a data-forwarding port from 0 - 65535.

```
otls forward [2.4GHz|5GHz] [disable|enable]
```

otls forward [2.4GHz|5GHz] [disable|enable]	Enables or disables OTLS tag forwarding • 2.4GHz – Enables or disables forwarding of OTLS beacons received on the 2.4 GHz band • 5GHz – Enables or disables forwarding of OTLS beacons received on the 5.0 GHz band The following keywords are common to the above parameters: • disable – Disables OTLS tag forwarding. By default OTLS beacon forwarding is disabled for both 2.4 GHz and 5.0 GHz bands. • enable – Enables OTLS tag forwarding

```
otls server-ip <OTLS-SERVER-IP>
```

otls server-ip <OTLS-SERVER-IP>	Configures the OTLS server's IP address • <OTLS-SERVER-IP> – Specify the OTLS server's IP address.

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

no on page 1214	Removes the OTLS-related parameters configured on an AP or on an AP's profile

offline-duration

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`offline-duration <5-43200>`

Parameters

```
offline-duration <5-43200>
```

offline-duration <5-43200>	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

no on page 1214	Resets the offline-duration to default (10 minutes)

power-config

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

power-config	Configures the power option mode
af-option [range|throughput]	Configures the 802.3.af power mode option. The options are: • range – Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains. 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. • throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. 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.
at-option [range|throughput]	Configures the 802.3 at power mode option. The options are: • range – Configures the at power range mode. This mode provides higher power but fewer tx chains. 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. • throughput – Configures the at power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. 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.

```
power-config mode [auto|3af]
```

power-config	Configures the power option mode
mode [auto|3af]	Configures the AP power mode • 3af – Forces an AP to power up in the 802.3af power mode • auto – Sets the detection auto mode (default setting) The automatic power-config mode enables an access point to automatically determine the best power configuration based on the available power budget.

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

no on page 1214	Reverts the power mode setting on this profile to default

preferred-controller-group

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
preferred-controller-group <WORD>
```

Parameters

```
preferred-controller-group <WORD>
```

<WORD>	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 pre
ferred-controller-group
 preferred-controller-group testGroup
NOC-NX9500(config-profile-testNX9000)#
```

Related Commands

no on page 1214	Removes the preferred controller group configuration

preferred-tunnel-controller

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
preferred-tunnel-controller <NAME>
```

Parameters

```
preferred-tunnel-controller <NAME>
```

preferred-tunnel-controller <NAME>	Configures the preferred tunnel name

Example

```
nx9500-6C8809(config-profile-default-rfs4000)#preferred-tunnel-controller testtunnel
```

Related Commands

no on page 1214	Removes the preferred tunnel configuration

purview-application-policy

Profile Config Commands on page 853

Enables the RADIUS *Change of Authorization* (CoA) mechanism. When enabled, successfully authenticated users are reauthenticated and the attributes of their active AAA session changed based on the rules defined by the Purview application policy specified here.

For information on configuring a Purview application policy, see purview-application-policy on page 436.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
purview-application-policy radius <PURVIEW-APP-POLICY-NAME>
```

Parameters

```
purview-application-policy radius <PURVIEW-APP-POLICY-NAME>
```

purview-application-policy radius <PURVIEW-APP-POLICY-NAME>	Applies a Purview application policy to a controller or access point profile or device • <PURVIEW-APP-POLICY-NAME> – Specify the Purview application policy name (should be existing and configured).

Example

```
nx9500-6C8809(config-profile-testNX9500)#purview-application-policy radius Social-Net

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include purview-
application-policy
 purview-application-policy radius Socila-Net
nx9500-6C8809(config-profile-testNX9500)#
```

Related Commands

no on page 1214	Removes the RADIUS-server provided application policy associated with this profile

radius

Profile Config Commands on page 853

Configures device level RADIUS authentication parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`radius [nas-identifier|nas-port-id] <WORD>`

Parameters

```
radius [nas-identifier|nas-port-id] <WORD>
```

radius	Configures RADIUS authentication parameters
nas-identifier <WORD>	Specifies the RADIUS Network Access Server (NAS) identifier attribute used by this device • <WORD> – Specifies the NAS identifier
nas-port-id <WORD>	Specifies the RADIUS NAS port ID attribute used by this device • <WORD> – Specifies the NAS port ID

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

no on page 1214	Disables or reverts settings to their default

rf-domain-manager

Profile Config Commands on page 853

Configures the RF Domain manager election criteria

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
rf-domain-manager [capable|priority <1-255>]
```

Parameters

```
rf-domain-manager [capable|priority <1-255>]
```

rf-domain-manager	Configures the RF Domain manager election criteria
capable	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.
priority <1-255>	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. • <1-255> – Select a priority value from 1 - 255.

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

no on page 1214	Disables or reverts settings to their default

router

Profile Config Commands on page 853

Enables dynamic routing (BGP and/or OSPF) and enters the routing protocol configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Note
BGP is supported only on RFS4000, NX7500, and NX9500 model controllers and service platforms.

The NX9500 service platforms do not support OSPF routing.

The access points only support OSPF routing.

Syntax

```
router [bgp|ospf]
```

Parameters

```
router [bgp|ospf]
```

router	Enables dynamic routing and enters the routing protocol configuration mode
bgp	Enables BGP dynamic routing and configures relevant settings BGP is an inter-ISP routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between AS *(Autonomous Systems)* 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. 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. For more information on dynamic BGP routing configurations, see Border Gateway Protocol on page 1867 .
ospf	Enables OSPF dynamic routing and configures relevant settings. Changes configuration mode to router mode 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. For more information on dynamic OSPF routing configurations, see Router Mode on page 1733.

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

no on page 1214	Disables OSPF settings

spanning-tree

Profile Config Commands on page 853

Enables spanning tree commands. Use these commands to configure the errdisable, multiple spanning tree and portfast settings.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

spanning-tree	Configures spanning-tree related parameters
errdisable	Disables or shuts down ports where traffic is looping, or ports with traffic in one direction
recovery	Enables the timeout mechanism for a port to be recovered. This option is disabled by default.
cause bpduguard	Specifies the reason for errdisable • bpduguard – Recovers from errdisable due to bpduguard
interval <10-1000000>	Specifies the interval after which a port is enabled • <10-1000000> – Specify a value from 10 - 1000000 seconds. The default is 300 seconds.

```
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	Configures spanning-tree related parameters
mst	Configures Multiple Spanning Tree (MST) commands 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.
<0-15> priority <0-61440>	Specifies the number of instances required to configure MST. Select a value from 0 -15. • 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. • <0-61440> – Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root)
cisco interoperability [enable|disable]	Enables CISCO interoperability Enables interoperability with CISCO's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
enable	Enables MST protocol
forward-time <4-30>	Specifies the forwarding delay time in seconds • <4-30> – Specify a value from 4 - 30 seconds. The default is 15 seconds.
hello-time <1-10>	Specifies the hello BDPU interval in seconds • <1-10> – Specify a value from 1 - 10 seconds. The default is 2 seconds.
instance <1-15>	Defines the instance ID to which the VLAN is associated • <1-15> – Specify an instance ID from 1 - 10.
max-age <6-40>	Defines the maximum time to listen for the root bridge • <6-40> – Specify a value from 4 - 60 seconds. The default is 20 seconds.
max-hops <7-127>	Defines the maximum hops when BPDU is valid • <7-127> – Specify a value from 7 - 127. The default is 20.
region <LINE>	Specifies the MST region • <LINE> – Specify the region name.
revision <0-255>	Sets the MST bridge revision number. This enables the retrieval of configuration information. • <0-255> – Specify a value from 0 - 255. This default is 0.

```
spanning-tree portfast [bpdufilter|bpduguard] default
```

spanning-tree	Configures spanning-tree related parameters
portfast [bpdufilter| bpduguard] default	Enables PortFast on a bridge • bpdufilter default – Sets the BPDU filter for the port. The BPDU filter is disabled by default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures that PortFast enabled ports do not transmit or receive BPDUs. • bpduguard default – Guards PortFast ports against BPDU receive. The BPDU guard is disabled by default. Enabling the BPDU guard means this port will shutdown on receiving a BPDU. • default – Enables the BPDU filter and/or BPDU guard on PortFast enabled ports by default

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

no on page 1214	Disables or reverts settings to their default

traffic-class-mapping

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

Parameters

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

traffic-class-mapping	Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority
<IPv6-TRAFFIC-CLASS-VALUE>	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.
priority <0-7>	Specify the 802.1p priority to map with the traffic-class value specified in the previous step • <0-7> – Specify a value from 0 - 7. 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: • 0 – Best Effort • 1 – Background • 2 – Spare • 3 – Excellent Effort • 4 – Controlled Load • 5 – Video • 6 – Voice • 7 – Network Control

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

no on page 1214	Removes mapping between IPv6 traffic class value (of incoming IPv6 untagged packets) and 802.1p priority

traffic-shape

Profile Config Commands on page 853

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 1238. And for configuring DSCP traffic class mappings, see dscp-mapping on page 986.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]
```

traffic-shape activation-criteria	Configures traffic-shape activation criteria that determines when the device invokes traffic shaping
always	Always invokes traffic shaping. This is the default setting.

cluster-master	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.
rf-domain-manager	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.
vrrp-master <1-255>	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. • <1-255> – Specify the VRRP group ID from 1 - 255.

```
traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>
```

traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>	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. • class <1-4> – Map the specified application category to a traffic-shaper class from 1 - 4. Note: app-category <APP-CATEGORY-NAME> – 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.
	Before configuring an application category to class mapping, ensure that the specified classes have been configured. Use the 'class > [max-buffers|max-latency|rate]' option available with this command to configure a traffic shaper class. For more information, see following parameter tables.

```
traffic-shape application <APPLICATION-NAME> class <1-4>
```

traffic-shape app-category <APPLICATION-NAME> class <1-4>	Configures an application to traffic-class mapping. Use this option to apply an application to traffic-shaper class mapping. • app-category <APPLICATION-NAME> – Specify the application name. • class <1-4> – Map the specified application to a traffic-shaper class from 1 - 4. Note: Before configuring an application to class mapping, ensure that the specified classes have been configured. Use the 'class > [max-buffers|max-latency|rate] option available with this command to configure a traffic shaper class. For more information, see following tables.

```
traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-100>}
```

traffic-shape class <1-4> max-buffers <1-400>	Configures the queue length limit for different traffic-shaper class • class <1-4> – Specify the traffic-shaper class from 1 - 4. • max-buffers <1-400> – Configures the maximum queue lengths for packets of different priority queues, after which the queue starts to drop packets. <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. Note: For access points the upper queue length limit is 400.
red-level <1-400>	Optional. Performs Random Early Drop (RED) when a specified queue length in packets is reached • <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. 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. Note: For more information on default values, see the Usage Guidelines section in this topic.
red-percent <1-100>	Optional. Performs RED when a specified value, which is a percentage of the max-buffers configured, is reached • <1-100> – Configure the percentage of the maxi-buffers from 1 - 100 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.

```
traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]
```

traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]	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. • class <1-4> – Specify the traffic-shaper class from 1 - 4. • max-latency <1-1000000> – Configures the max-latency for packets of different priority queues, after which the queue starts to drop packets. <1-1000000> – Configure the max-latency from 1 - 100000 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. [msec|usec] – Configures the unit for measuring latency as milliseconds (msec) or microseconds (usec). The default setting is msec.

```
traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-100>]
```

traffic-shape class <1-4> rate	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. • class <1-4> – Specify the traffic-shaper class from 1 - 4.
<1-250000> [Kbps|Mbps]	Configures the traffic rate, in Kbps, Mbps, for the class specified in the previous step • <1-250000> – Specify the rate from 1 - 250000. • [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Kbps. Note: The range varies depending on the unit selected. It is 1 - 250 Mbps, or 250 - 250000 Kbps.
total-bandwidth-percent <1-100>	Configures the traffic rate, as a percentage of the total available bandwidth, for the class specified in the previous first step • <1-100> – Specify the traffic rate from 1 - 100% of the total bandwidth.

```
traffic-shape priority-map <0-7>
```

traffic-shape priority-map <0-7>	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. • priority-map <0-7> – Specify the priority from 0 - 7 for priority levels 0, 1, 2, 3, 4, 5, 6, and 7. 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.

```
traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]
```

traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]	Configures the total-bandwidth for traffic shaping • <1-1000000> – Specify the value from 1 - 1000000 Kbps/Mbps. The default value is 10 Mbps. • [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Mbps. Note: The range varies depending on the unit selected. It is 1 - 1000 Mbps, or 250 - 1000000 Kbps.

```
traffic-shape enable
```

traffic-shape enable	Enables traffic shaping using the defined bandwidth, rate and class mappings configured using this command **Note:** Traffic shaping is disabled by default.

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

no on page 1214	Removes traffic shaping configuration or reverts them to the default values

trustpoint (profile-config-mode)

Profile Config Commands on page 853

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 1300.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

trustpoint	Assigns an existing trustpoint to validate CMP auth operator, client certificates, and RADIUS server certificate
https	Assigns an existing trustpoint to validate HTTPS requests

cmp-auth-operator	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.
radius-ca	Assigns an existing trustpoint to validate client certificates in EAP
radius-server	Assigns an existing trustpoint to validate RADIUS server certificate
<TRUSTPOINT-NAME>	The following keyword is common to all of the above parameters: • <TRUSTPOINT-NAME> – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device).

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

no on page 1214	Removes trustpoint-related configurations

tunnel-controller

Profile Config Commands on page 853

Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`tunnel-controller <NAME>`

Parameters

```
tunnel-controller <NAME>
```

tunnel-controller <NAME>	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name • <NAME> – Specify the name.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#tunnel-controller testGroup
```

Related Commands

no on page 1214	Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform's name

use (profile/device-config-mode-commands)

Profile Config Commands on page 853

Associates existing policies with this profile. This command is also applicable to the device configuration mode.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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-
policyip-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>
```

use	Associates the specified policies with this profile The specified policies should be existing and configured.
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.
bonjour-gw-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Forwarding policy name (should be existing and configured). For more information on Bonjour GW Forwarding policy, see bonjour-gw-forwarding-policy on page 223.
bonjour-gw-query-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Query Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal with this profile • <CAPTIVE-PORTAL> – Specify the captive portal name.
client-identity-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this profile • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see client-identity on page 271 and client-identity-group on page 277.
crypto-cmp-policy <POLICY-NAME>	Associates an existing crypto certificate management protocol (CMP) policy with this profile • <POLICY-NAME> – Specify the CMP policy name. For more information on configuring a crypto CMP policy, see Crypto-CMP Policy on page 1846.
database-client-policy <POLICY-NAME>	Associates an existing database client policy with a profile • <POLICY-NAME> – Specify the policy name (should be existing and configured). For more information on database client policy, see database-client-policy global-config on page 296. Applicable only to the NX9500, NX9600, and VX9000 model service platforms.

dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-POLICY> – Specify the DHCP server policy name.
dhcpv6-server-policy <DHCPv6-POLICY>	Associates a DHCPv6 server policy • <DHCPv6-POLICY> – Specify the DHCPv6 server policy name.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-association-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the controller profile • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. 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 global-association-list on page 367.
guest-management <GUEST-MANAGEMENT-POLICY-NAME>	Associates the specified guest management policy with the controller profile • <GUEST-MANAGEMENT-POLICY-NAME> – Specify the guest management policy name (should be existing and configured).
iot-device-type-imagotag-policy <POLICY-NAME>	Associates an IoT Imago Tag policy to an AP's profile or device context. • <POLICY-NAME> – 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 AP8432 model access points.
ip/ipv6-access-list <IP/IPv6-ACL-NAME> traffic-shape class <1-4>	Associates an IP and/or IPv6 ACL with this profile and applies it as a firewall for the selected traffic-shape class • <IP/IPv6-ACL-NAME> – Specify the IP/IPv6 ACL name (should be existing and configured) • traffic-shape class <1-4> – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL <1-4> – Select the traffic-shape class from 1 - 4.
location-policy <POLICY-NAME>	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. It is applicable to the following platform profiles: RFS4000, NX5500, NX7500, NX9500, NX9600, and VX9000. • <POLICY-NAME> – Specify the policy name.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.

role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.
web-filter-policy <POLICY-NAME>	Associates an existing Web Filter policy with a profile or device • <POLICY-NAME> – Specify the policy name.

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>
```

use	Associates the following policies with this device:
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.
bonjour-gw-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Forwarding policy name (should be existing and configured). For more information on Bonjour GW Forwarding policy, see bonjour-gw-forwarding-policy on page 223.
bonjour-gw-query-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Query Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal • <CAPTIVE-PORTAL> – Specify the captive portal name.
client-identity-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this device • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see client-identity on page 271 and client-identity-group on page 277.
crypto-cmp-policy <POLICY-NAME>	Associates an existing crypto certificate management protocol (CMP) policy • <POLICY-NAME> – Specify the CMP policy name. For more information on configuring a crypto CMP policy, see Crypto-CMP Policy on page 1846.
database-client-policy <POLICY-NAME>	Associates an existing database client policy with a device • <POLICY-NAME> – Specify the policy name (should be existing and configured). For more information on database client policy, see database-client-policy global-config on page 296. Applicable only to the NX9500, NX9600, and VX9000 model service platforms.

database-policy <DATABASE-POLICY-NAME>	Associates an existing database policy with this device • <DATABASE-POLICY-NAME> – Specify the database policy name. **Note:** For more information on configuring a database policy, see database-policy global config on page 299.
dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-POLICY> – Specify the DHCP server policy name.
dhcpv6-server-policy <DHCPv6-POLICY>	Associates a DHCPv6 server policy • <DHCPv6-POLICY> – Specify the DHCPv6 server policy name.
enterprise-ui	Enables application of the site controller's Enterprise user interface (UI) on all management points (controllers and access points) For example, the site controller is NX 5500 and an AP 7562 is adopted to it. To enable the access point to also use the Enterprise UI: On the AP 7562's profile configuration mode execute: `use > enterprise-ui` On adoption and application of this profile, the AP 7562 access point resets and reboots using the Enterprise UI. Once using the Enterprise UI, on all subsequent adoptions, the AP does not get reset.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-association-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the device (controller) • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. Once associated, the controller applies this association list to requests received from all adopted APs. For more information on global association list, see global-association-list on page 367.
guest-management <GUEST-MANAGEMENT-POLICY-NAME>	Associates the specified guest management policy with this device • <GUEST-MANAGEMENT-POLICY-NAME> – Specify the guest management policy name (should be existing and configured).
ip/ipv6-access-list <IP/IPv6-ACL-NAME> traffic-shape class <1-4>	Associates an IP and/or IPv6 ACL with this device and applies it as a firewall for a selected traffic-shape class • <IP/IPv6-ACL-NAME> – Specify the IP/IPv6 ACL name (should be existing and configured) • traffic-shape class <1-4> – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL <1-4> – Select the traffic-shape class from 1 - 4.
license <WORD>	Associates a Web filtering license with this device • <WORD> – 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.

location-policy <POLICY-NAME>	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. It is applicable to the following platform profiles: AP-7522, AP 7532, AP 7562, AP 7602, AP-7612, AP 7622, AP7632, AP7662, AP-8432, AP-8533, RFS 4000, NX 5500, NX 7510, NX 95XX, NX 96XX, and VX 9000 . • <POLICY-NAME> – Specify the policy name.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
nsight-policy <NSIGHT-POLICY-NAME>	Associates a specified NSight policy with this device • <NSIGHT-POLICY-NAME> – Specify the NSight policy name (should be existing and configured). **Note:** Use this command to associate an NSight policy to a controller to enable it to function as the NSight server. For more information, see nsight-policy (global-config-mode) on page 418.
profile <PROFILE-NAME>	Associates a profile with this device • <PROFILE-NAME> – Specify the profile name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.
rf-domain <RF-DOMAIN-NAME>	Associates an RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.
rtl-server-policy <POLICY-NAME>	Associates a RTL *(Real TIme Locationing)* server policy with an access point. When associated, enables the access point to directly send RSSI feeds to the third-party Euclid RTL server. • <POLICY-NAME> – Specify the RTL server policy name (should be existing and configured).
sensor-policy <POLICY-NAME>	Associates a sensor policy with an access point or controller. When associated, WiNG controllers and access points function as sensors. • <POLICY-NAME> – Specify the sensor policy name (should be existing and configured).
wips-policy <WIPS-POLICY>	Associates a WIPS policy • <WIPS-POLICY> – Specify the WIPS policy name.
web-filter-policy <POLICY-NAME>	Associates an existing Web Filter policy with a profile or device • <POLICY-NAME> – Specify the policy name.

```
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

no on page 1214	Disassociates a specified policy from this profile/device

vrrp

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
delta-priority <1-253>	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. • <1-253> – Specify the delta priority level from 1- 253.
description <LINE>	Configures a text description for the virtual router to further distinguish it from other routers with similar configuration • <LINE> – Provide a description (a string from 1- 64 characters in length)

ip <IP-ADDRESSES>	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. • <IP-ADDRESSES> – Specify the IP address(es) in the A.B.C.D format. This configuration triggers VRRP operation.
preempt {delay <1-65535>}	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. • 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.
priority <1-254>	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).
sync-group	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>
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
interface vlan <1-4094>	Enables VRRP on the specified switch VLAN interface (SVI) • vlan <1-4094> – Specify the VLAN interface ID from 1 - 4094.

```
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>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
monitor	Enables link monitoring or Critical Resource Monitoring (CRM)
critical-resource <CRM-NAME1>	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.
action [decrement-priority| increment-priority]	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. • decrement-priority – Decrements the priority of virtual router on critical resource down event • increment-priority – Increments the priority of virtual router on critical resource down event
<IF-NAME>	Optional. Enables interface monitoring • <IF-NAME> – Specify the interface name to monitor
pppoe1	Optional. Enables Point-to-Point Protocol (PPP) over Ethernet interface monitoring

vlan <1-4094>	Optional. Enables VLAN (switched virtual interface) interface monitoring • <1-4094> – Specify the VLAN interface ID from 1- 4094.
wwan1	Optional. Enables Wireless WAN interface monitoring

```
vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
timers	Configures the timer that runs every interval
advertise [<1-255>| centiseconds <25-4095>| msec <250-999>]	Configures the VRRP advertisements time interval. This is the interval at which a master sends out advertisements on each of its configured VLANs. • <1-255> – Configures the timer interval from 1- 255 seconds. (applicable for VRRP version 2 only) • centiseconds <25-4095> – Configures the timer interval in centiseconds (1/100th of a second). Specify a value between 25 - 4095 centiseconds (applicable for VRRP version 3 only). • msec <250-999> – Configures the timer interval in milliseconds (1/1000th of a second). Specify a value between 250 - 999 msec (applicable for VRRP version 2 only). Default is 1 second.

```
vrrp version [2|3]
```

vrrp version [2|3]	Configures one of the following VRRP versions: • 2 – VRRP version 2 (RFC 3768). This is the default setting. • 3 – VRRP version 3 (RFC 5798 only IPV4) The VRRP version determines the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.

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
 vrrp 1 preempt
 vrrp 1 sync-group
 vrrp 1 delta-priority 100
 vrrp version 3
nx9500-6C8809(config-profile-default-rfs4000)#
```

Related Commands

no on page 1214	Reverts VRRP settings

vrrp-state-check

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
vrrp-state-check
```

Parameters

None

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#vrrp-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
 vrrp-state-check
 controller adopted-devices controllers
 alias string $SN B4C7996C8809
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no on page 1214	Disables the publishing of an interface via OSPF/BGP based on VRRP status

wep-shared-key-auth

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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 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

no on page 1214	Disables support for 802.11 WEP shared key authentication

ws-controller

Profile Config Commands on page 853

This parameter allows WiNG APs adopted to ExtremeCloud Appliance to rediscover a new controller in case the first controller is unreachable. It applies to WiNG APs configured to adopt to a WebSocket controller (ExtremeCloud Appliance). In other words, the AP's adoption-mode on page 858 is set to 'ws-controller'.

As per the current implementation, WiNG AP adoption to the ExtremeCloud Appliance WebSocket controller, supports only one controller. If the adopting controller goes down, the AP does not attempt to re-discover and adopt to another controller. If the AP reboots, it uses the management-server configuration to discover and adopt to the first discovered controller. This prevents the AP from adopting to a new controller. Use this parameter to configure multiple ws-controller hosts and enable rediscovery of new ws-controller.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ws-controller host <1-5> port <1-65535>
```

Parameters

```
ws-controller <1-5> port <1-65535>
```

ws-controller host <1-5>	Configures multiple WebSocket controller hosts. • <1-5> - Select the controller to configure. A maximum of five controllers can be configured. When a WiNG AP with adoption-mode set to 'ws-controller' reboots, it will try to connect to the ws-controller received in DHCP option 191, then it will try connecting to the controller hosts configured here.
port <1-65535>	Specify the port on which the controller is reachable. • <1-65535> - Select the port number from 1 to 65535. The default value is 443.

Examples

```
nx9500-6C8809(config-profile-test8432)#ws-controller 1 host 1.2.3.4 port 100
nx9500-6C8809(config-profile-test8432)#show context  include-factory | include ws-
controller
 ws-controller 1 host 1.2.3.4 port 100
nx9500-6C8809(config-profile-test8432)#
```

Related Commands

no on page 1214	Reverts the adoption-mode to default (controller)

service

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, 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-deauth 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>
```

captive-portal-server connections-per-ip <3-64>	Configures the maximum number of simultaneous captive portal connection allowed per IP address • <3-64> – Specify the maximum number of connections per IP address from 3 - 64. The default is 3. Note: This command is applicable only to the NX9XXX and NX9600 service platform profiles.

```
service cluster master-election immediate
```

cluster master-election immediate	Initiates and completes cluster master election as soon as just one cluster member comes on and is active. This option is disabled by default.

```
service critical-resource port-mode-source-ip <IP>
```

critical-resource port-mode-source-ip <IP>	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.

```
service enable [l2tpv3|pppoe|radiusd]
```

service enable l2tpv3	Enables L2TPv3 on this profile
service enable pppoe	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.
service enable radiusd	Enables RADIUSD features. When executed on a device, enables RADIUSD on the logged device. When executed on a profile, enables RADIUSD on all devices using that profile.

```
service global-association-list blacklist-interval <1-65535>
```

service global-association-list	Configures global association list related parameters
blacklist-interval <1-65535>	Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server. • <1-65535> – Specify a value from 1 - 65535 seconds. The default is 60 seconds.

```
service lldp loop-detection
```

lldp loop-detection	Enables network loop detection via LLDP. This option is disabled by default.

```
service memory kernel decrease
```

service memory kernel decrease	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. This option is disabled by default.

```
service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-4>| port-channel <1-2>]
```

meshpoint loop-prevention-port	Limits meshpoint loop prevention to a single port
<L2-INTERFACE-NAME>	Limits meshpoint loop prevention on a specified Ethernet interface • <L2-INTERFACE-NAME> – Specify the layer 2 Ethernet interface name.
ge <1-4>	Limits meshpoint loop prevention on a specified GigabitEthernet interface • ge <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
port-channel <1-2>	Limits meshpoint loop prevention on a specified port-channel interface • port-channel <1-2> – Specify the port-channel interface index from 1 - 2.

```
service pm sys-restart
```

pm sys-restart	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]
```

power-config 3af-out	Enables LLDP power negotiation, but uses 3af power. This option is disabled by default.
power-config force-3at	Disables LLDP negotiation and forces 802.3at power configuration. This option is disabled by default.

```
service radius dynamic-authorization additional-port <1-65535>
```

radius dynamic-authorization additional-port <1-65535>	Configures an additional UDP port used by the device to listen for dynamic authorization messages • <1-65535> – Specify a value from 1 - 65535. The default is 3799. The Cisco Identity Services Engine (ISE) server uses port 1700.

```
service remote-config apply-delay <0-600>
```

remote-config apply-delay <0-600>	Delays configuration of a remote device (after it becomes active) by the specified time period • <0-600> – Specify a value from 0 - 600 seconds. The default is 0 seconds.

```
service rss-timeout <0-86400>
```

rss-timeout <0-86400>	Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after loosing controller adoption. • <0-86400> – Specify a value from 0 - 86400 seconds. The default is 300 seconds.

```
service watchdog
```

watchdog	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
```

wireless anqp-frag-always	Enables fragmentation of all ANQP packets. This option is disabled by default.

```
service wireless anqp-frag-size <100-1500>
```

wireless anqp-frag-size <100-1500>	Configures the ANQP packet fragment size • <100-1500> – Specify a value from 100 - 1500. The default is 1200.

```
service wireless client tx-deauth on-radar-detection
```

wireless client	Configures wireless client and stations related settings
tx-deauth on-radar-detection	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]
```

wireless cred-cache-sync	Configures the credential cache's synchronization parameters. The parameters are: full, interval, never, and partial.
full	Enables synchronization of all credential cache entries
interval <30-864000>	Sets the interval, in seconds, at which the credential cache is synchronized • <30-864000> – Specify a value from 30 - 864000 seconds. The default is 1200 seconds.
never	Disables credential cache entry synchronization for all associated clients other than roaming clients. This is the default setting.
partial	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>]
```

wireless inter-ap-key	Configure encryption key used for securing inter-ap messages. This option is disabled by default.
[0<WORD>| 2<WORD>| <WORD>]	Specify a clear text or encrypted key.

```
service wireless noise-immunity
```

wireless noise-immunity	Polls for status and reconfigures radio in case of receive stall. This option is enabled by default.

```
service wireless reconfig-on-rx-stall
```

wireless reconfig-on-rx-stall	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]
```

wireless test	Configures the serviceability parameters used for testing
[max-rate|min-rate]	Configures the maximum and minimum data rates for clients using rate-scaling. The 'max-rate' and min-rate' options are disabled by default.
[1,2,5.5,....mcs23]	Select the maximum and minimum data rates applicable.

```
service wireless test max-retries <0-15>
```

wireless test	Configures the serviceability parameters used for testing
max-retries <0-15>	Configures the maximum number of retries per packet from 0 - 15. The default is 0.

```
service wireless wispe-controller-port <1-65535>
```

wispe-controller-port <1-65535>	Resets the WIreless Switch Protocol Enhanced (WISPe) controller port. This is the UDP port used to listen for WISPe. • <1-65535> – Specify a value from 1 - 65535. The default is 24756.

```
service show cli
```

show cli	Displays running system configuration details • cli – Displays the CLI tree of the current mode

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

no on page 1214	Removes or resets service command parameters

zone

Profile Config Commands on page 853

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`zone <NAME>`

Parameters

```
zone <NAME>
```

zone <NAME>	Configures the device's zone/area • <NAME> – Specify the zone/areaname.

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

no on page 1214	Removes the zone configured on this profile or device

Device Config Commands

Profiles on page 848

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
adopter-auto-provisioning-policy-lookup on page 857	Enables the use of a centralized auto provisioning policy on this device
adoption on page 857	Configures a minimum and maximum delay time in the initiation of the device adoption process
adoption-site on page 1272	Sets the device's adoption site name
alias on page 865	Configures network, VLAN, and service aliases on a device
application-policy on page 875	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.
area on page 1272	Sets the name of area where the system is deployed
arp on page 877	Configures ARP parameters

Command	Description
auto-learn on page 879	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.
autogen-uniqueid on page 880	When executed in the device configuration mode, this command generates a unique ID for the logged device
autoinstall on page 881	Autoinstalls firmware image and configuration setup parameters
bridge on page 883	Configures Ethernet Bridging parameters
captive-portal on page 910	Configures captive portal advanced Web page upload on this profile
cdp on page 911	Operates CDP on the device
channel-list on page 1273	Configures channel list advertised to wireless clients
cluster on page 912	Sets cluster configuration
configuration-persistence on page 914	Enables configuration persistence across reloads
contact on page 1274	Sets contact information
controller on page 915	Configures a WLAN's wireless controller or service platform
country-code on page 1275	Configures wireless controller or service platform's country code
critical-resource on page 920	Monitors user configured IP addresses and logs their status
crypto on page 929	Configures data encryption protocols and settings
database on page 976	Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value
device-upgrade on page 978	Configures device firmware upgrade settings on this device
diag on page 980	Enables looped packet logging
dot1x on page 981	Configures 802.1x standard authentication controls
dpi on page 983	Enables Deep Packet Inspection (DPI) on this device
dscp-mapping on page 986	Configures IP Differentiated Services Code Point (DSCP) to 802.1p priority mapping for untagged frames
eguest-server (VX9000 only) on page 987	Enables the EGuest daemon when executed without the 'host' option
eguest-server (NOC Only) on page 988	Points to the EGuest server, when executed along with the 'host' option
email-notification on page 989	Configures e-mail notification settings
enforce-version on page 991	Checks the device firmware version before attempting connection
environmental-sensor on page 992	Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configure its settings.
events on page 994	Enables system event message generation and forwarding
export on page 994	Enables export of startup.log file after every boot
file-sync on page 995	Configures parameters enabling syncing of trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points
floor on page 1276	Sets the floor name where the system is located

Command	Description
geo-coordinates on page 1277	Configures the geographic coordinates for this device
gre on page 997	Enables GRE tunneling on this device
hostname on page 1278	Sets a system's network name
http-analyze on page 1007	Enables HTTP analysis on this device
interface on page 1010	Selects an interface to configure
ip on page 1167	Configures IPv4 components
ipv6 on page 1175	Configures IPv6 components
l2tpv3 on page 1180	Defines the Layer 2 Tunnel Protocol (L2TP) protocol for tunneling Layer 2 payloads using Virtual Private Networks (VPNs)
l3e-lite-table on page 1182	Configures L3e Lite Table with this profile
lacp on page 1279	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.
layout-coordinates on page 1279	Configures layout coordinates
led on page 1183	Turns LEDs on or off
led-timeout on page 1184	Configures the LED-timeout timer in the device or profile configuration mode
legacy-auto-downgrade on page 1185	Enables legacy device firmware to auto downgrade
legacy-auto-update on page 1185	Auto updates AP7161 legacy device firmware
license on page 1280	Adds device feature licenses
lldp on page 1186	Configures Link Layer Discovery Protocol (LLDP) settings for this device
load-balancing on page 1187	Configures load balancing parameters.
location on page 1283	Configures the system's location (place of deployment)
location-server on page 1284	Configures the ExtremeLocation server's hostname in the AP's device context.
location-tenantid on page 1286	Configures the ExtremeLocation Tenant's account number in the selected AP's device context.
logging on page 1193	Enables message logging
mac-address-table on page 1195	Configures the MAC address table
mac-auth on page 1197	Enables 802.1x authentication of hosts on this device
mac-name on page 1286	Configures MAC address to device name mappings
management-server on page 1199	Configures a management server with this profile
meshpoint-device on page 1200	Configures meshpoint device parameters
meshpoint-monitor-interval on page 1201	Configures meshpoint monitoring interval
min-misconfiguration-recovery-time on page 1202	Configures the minimum device connectivity verification time
mint on page 1203	Configures MiNT protocol settings

Command	Description
misconfiguration-recovery-time on page 1211	Verifies device connectivity after a configuration is received
neighbor-inactivity-timeout on page 1212	Configures neighbor inactivity timeout value
neighbor-info-interval on page 1213	Configures the neighbor information exchange interval
no on page 1287	Negates a command or resets values to their default settings
noc on page 1216	Configures NOC settings
nsight on page 1288	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.
ntp on page 1221	Configures NTP server settings
offline-duration on page 1226	Sets the duration, in minutes, for which a device remains unadopted before it generates offline event
override-wlan on page 1293	Configures WLAN RF Domain level overrides on the logged device
power-config on page 1227	Configures power mode features
preferred-controller-group on page 1229	Specifies the wireless controller or service platform group the system prefers for adoption
preferred-tunnel-controller on page 1230	Configures the tunnel wireless controller or service platform preferred by the system for tunneling extended VLAN traffic
radius on page 1231	Configures device-level RADIUS authentication parameters
remove-override on page 1295	Removes device overrides
rf-domain-manager on page 1232	Enables the RF Domain manager
router on page 1233	Configures dynamic router protocol settings.
rsa-key on page 1297	Assigns a RSA key to SSH
sensor-server on page 1298	Configures an AirDefense sensor server
spanning-tree on page 1235	Enables spanning tree commands on the logged device
traffic-class-mapping on page 1238	Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority
traffic-shape on page 1239	Enables traffic shaping and configures traffic shaping parameters on this device
trustpoint (device-config-mode) on page 1300	Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server, etc.
timezone on page 1299	Configures wireless controller or service platform's time zone settings
tunnel-controller on page 1246	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name
use (profile/device-config-mode-commands) on page 1247	Associates different policies and settings with this device
vrrp on page 1253	Configures VRRP group settings

Command	Description
vrrp-state-check on page 1257	Publishes interface via OSPF or BGP based on Virtual Router Redundancy Protocol (VRRP) status
wep-shared-key-auth on page 1257	Enables support for 802.11 WEP shared key authentication
raid on page 1301	Enables alarm on the array. This command is supported only on the NX9500 series service platform.

adoption-site

Device Config Commands on page 1265

Sets the device's adoption site name

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
adoption-site <SITE-NAME>
```

Parameters

```
adoption-site <SITE-NAME>
```

adoption-site <SITE-NAME>	Sets the device's adoption site name

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#adoption-site SanJoseMainOffice
```

Related Commands

no on page 1287	Disables or reverts settings to their default

area

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
area <AREA-NAME>
```

Parameters

```
area <AREA-NAME>
```

area <AREA-NAME>	Sets the physical area where the device is deployed <AREA-NAME> – Specify the area name (should not 64 characters in length).

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#area RMZEcoSpace

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
apr505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname ap505-133E1C
 area RMZEcospace
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Disables or reverts settings to their default

channel-list

Device Config Commands on page 1265

Configures the channel list advertised to wireless clients

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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]
```

channel-list	Configures the channel list advertised to wireless clients
2.4GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 2.4 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.

5GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 5.0 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.
dynamic	Enables dynamic (neighboring access point based) update of configured channel list

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C))#channel-list 2.4GHz 1,2

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C))#show context
ap505 94-9B-2C-13-3E-1C)
 use profile default-ap505
 use rf-domain default
 hostname ap505-133E1C
 area RMZEcospace
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C))#
```

Related Commands

no on page 1287	Resets the channel list configuration

contact

Device Config Commands on page 1265

Defines an administrative contact for a deployed device (controller, service platform, or access point)

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`contact <WORD>`

Parameters

```
contact <WORD>
```

contact <WORD>	Specify the administrative contact name (should not exceed 64 characters in length)

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#contact Bob+1-631-738-5200

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname ap505-133E1C
 area RMZEcospace
```

```
 contact Bob+1-631-738-5200
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Resets the administrative contact name

country-code

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
country-code <WORD>
```

Parameters

```
country-code <COUNTRY-CODE>
```

country-code <COUNTRY-CODE>	Defines the two-digit country code for legal device deployment
	• <COUNTRY-CODE> – Specify the two letter ISO-3166 country code.
	
	Note: Alternately, press [TAB] to view the list of country codes supported. WiNG 7.1 supports 171 country codes.
	
	`ap505-13403B(config-device-94-9B-2C-13-40-38)#country-code`
	`Display all 171 possibilities? (y or n)`
	`ae ag ai al an ar at au ba bb bd be bf bg`
	`bh bj bm bn bo bq`
	`br bs bw by ca ch cl cm cn co cr cw cx cy`
	`cz de dk do dz ec`
	`ee eg es fi fk fm fr g1 g2 g3 g4 g5 g6 g7`
	`gb gd ge gf gh gp`
	`gr gt gy hk hm hn hr ht hu id ie in io iq`
	`ir is it jm jo jp`
	`--More--`
	`ap505-13403B(config-device-94-9B-2C-13-40-38)#`

Example

```
ap505-13403B(config-device-94-9B-2C-13-40-38)#country-code us
ap505-13403B(config-device-94-9B-2C-13-40-38)#show context include-factory | inc
lude country-code
```

```
 country-code us
ap505-13403B(config-device-94-9B-2C-13-40-38)#
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#country-code us

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname ap505-133E1C
 area RMZEcospace
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes the configured country code

floor

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`floor <FLOOR-NAME> <1-4094>`

Parameters

```
floor <FLOOR-NAME> <1-4094>
```

floor <FLOOR-NAME> <1-4094>	Sets the building floor name where the device is deployed • <1-4094> – 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.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#floor 5thfloor

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname ap505-133E1C
```

```
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes device's location floor name

geo-coordinates

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>`

Parameters

```
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

geographic coordinates	Configures the geographic coordinates for this device • <-90.0000-90.0000> – 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. • <-180.0000-180.0000> – 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.

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 ge1
  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

no on page 1287	Removes device's geographic coordinates

hostname

Device Config Commands on page 1265

Sets the system's network name

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`hostname <WORD>`

Parameters

```
hostname <WORD>
```

hostname <WORD>	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-94-9B-2C-13-3E-1C)#hostname TechPubAP505

The hostname has changed from 'ap505-133E1C' to 'TechPubAP505'

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-1-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
nx9500-6C8809((config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes device's hostname

lacp

Device Config Commands 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 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 1027 and lacp-channel-group on page 1028.

Supported in the following platforms:

- Service Platforms — NX5500, NX7500, NX9500, 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 1287	Removes this device's configured system-priority value

layout-coordinates

Device Config Commands on page 1265

Configures X and Y layout coordinates for the device

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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-94-9B-2C-13-3E-1C)#layout-coordinates 1.0 2.0

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes device's layout co-ordinates

license

Device Config Commands on page 1265

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/NSIGHT-PER/TRON)

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. 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
license <WORD> <LICENSE-KEY>
```

Parameters

```
license <WORD> <LICENSE-KEY>
```

<WORD>	Specify the feature name (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/ NSIGHT-PER/TRON) for which license is added. • 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. • 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. • 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. • HTANLT: This is the license key required to install Analytics (an enhanced statistical management tool) for NX9500 and NX9600 series service platforms. • 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. • 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. 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. **Note:** NSight is supported only on NX9500, NX9600 model service platforms, and the VX9000 virtual controller. • TRON – TRON is a proprietary FedEx BLE asset tracking application that tracks tagged packages moving through a distribution center. This license enables the TRON-feature entitlement on TRON-capable, WiNG APs. It is applied on the self of the controller adopting the APs. TRON-tracking is turned on when a TRON-capable vWiNG AP, having the requisite initial configurations, adopts to a controller having the TRON license. The license does not put a limit on the AP count. In other words, the license enables TRON feature entitlement for all TRON-capable APs, adopting to the controller. For more information on setting the initial configurations, see tron on page 1161 . **Note:**

	TRON-tracking is supported only on the AP8533 model access point. The license can be applied only on the NX5500, NX7500, NX9500, NX9600, and VX9000 platforms.
<LICENSE-KEY>	Specify the license key.

Examples

```
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#license AAP 66069c24b3bb1259b34ff016
c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#license AP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7164a1b1e51df2cc87902c9ae7281d319
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#license NSIGHT
66069c24b3bb12596b3d07672fdf5ccc99dd408f0ff891e719a98e92028e10e7a7461de1b5e70f32
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#license HOTSPOT-ANALYTICS
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#show licenses
Serial Number : B4C7996C8809

Device Licenses:
  AP-LICENSE
    String     :
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7164a1b1e51df2cc87902c9ae7281d319
    Value      : 256
    Borrowed   : 0
    Total      : 256
    Used       : 0
  AAP-LICENSE
    String     :
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
    Value      : 10250
    Borrowed   : 0
    Total      : 10249
    Used       : 2
  HOTSPOT-ANALYTICS
    String     :
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
  NSIGHT
    String     :
66069c24b3bb12596b3d07672fdf5ccc99dd408f0ff891e719a98e92028e10e7a7461de1b5e70f32
    Value      : 50
NOC-NX9500(config-device-B4-C7-99-6C-88-09)#
```

location

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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-94-9B-2C-13-3E-1C)#location SanJose

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes a managed device's location

location-server

Device Config Commands on page 1265

Configures the ExtremeLocation server's hostname on the AP. When configured, the access point uses a Websocket, to forward 802.11 frames and BLE beacons to the specified ExtremeLocation server.

Starting with WiNG 7.1.2, AP5XX APs will not use WIPS to collect WiFi packets and BLE (iBeacons and Eddystone) beacons. The information will be collected in the Collector Table and forwarded to the ExtremeLocation server from the Collector Table.

Note

The AP's radio should be in the radio-share or sensor mode and the AP's BLE radio should be in the le-sensor mode.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
location-server 1 ip <HOSTNAME> {port <1-65535>}
```

Parameters

```
location-server 1 ip <HOSTNAME> {port <1-65535>}
```

location-server 1 ip <HOSTNAMEL>	Identifies the ExtremeLocation server by its hostname • 1 – Sets the server ID as 1. As of now only one ExtremeLocation server is configurable. • ip <HOSTNAME> – Enter ExtremeLocation server's hostname. This is the ExtremeLocation server designated to receive RSSI scan data from a WiNG dedicated sensor. **Note:** 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.
port <1-65535>	Optional. Configures the port where the ExtremeLocation server is reachable. • <1-65535> – Specify a port from 1 - 65535. **Note:** By default, the ExtremeLocation server is reachable on port 443.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#location-server 1 ip
feeds.extremelocation.com
 port 200

nx9500-6C8809(config-device-94-9B-2C-13-40-38)#show context include-factory | include
location-server
 location-server 1 ip test port feeds.extremelocation.com
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#
```

Enabling Data forwarding to the ExtremeLocation Server

1 Configure sensor policy.

```
nx9500-6C8809(config-sensor-policy-ble)#rssi-interval-duration 35
```

2 In the AP's device context:

a Use the sensor policy.

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#use sensor-policy ble
```

b Configure the ExtremeLocation server hostname.

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#location-server 1 ip
feeds.extremelocation.com
```

c Configure the ExtremeLocation TenantID.

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#location-tenantid 1234
```

Related Commands

no on page 1287	Removes the ExtremeLocation server configuration.

location-tenantid

Device Config Commands on page 1265

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 on the AP. When configured, data (802.11 frames and/or BLE beacons) 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.

For information on enabling data forwarding to the ExtremeLocation server, see location-server on page 1284.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
location-tenantid <WORD>
```

Parameters

```
location-tenantid <WORD>
```

location-tenantid <WORD>	Configures the ExtremeLocation Tenant's account number • <WORD> – Specify the account number.

Examples

```
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#location-tenantid 123456
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#show context
ap505 94-9B-2C-13-40-38
 use profile default-ap505
 use rf-domain default
 hostname ap505-134038
 no staging-config-learnt
 location-server 1 ip test port 200
 location-tenantid 123456
nx9500-6C8809(config-device-94-9B-2C-13-40-38)#
```

Related Commands

no on page 1287	Removes the ExtremeLocation Tenant's account number configuration

mac-name

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mac-name <MAC> <NAME>
```

Parameters

```
mac-name <MAC> <NAME>
```

mac-name <MAC> <NAME>	Maps a user-friendly name to the device's MAC address • <MAC> – Specify the device's MAC address. • <NAME> – Specify the 'friendly' name used for the specified MAC address. This is the name used in events and statistics logs.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#mac-name 00-04-96-4A-A7-08 5.8TestAP

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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 94-9B-2C-13-3E-1C 5.8TestAP
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes the device's friendly name to MAC address mapping

no

Device Config Commands on page 1265

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

no <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

```
ap505-13403B(config-device-94-9B-2C-13-40-38)#no area

ap505-13403B(config-device-94-9B-2C-13-40-38)#no contact
```

nsight

Device Config Commands on page 1265

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 1291.

Configure these parameters in the NSight server's device configuration mode.

Supported in the following platforms:

- Service Platforms — NX9500, 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]
```

nsight database statistics	Configures NSight database statistics related parameters
avc-update-interval	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 Usage Guidelines (Data Aggregation and Expiration) on page 1291. 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.
update-interval	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 Usage Guidelines (Data Aggregation and Expiration) on page 1291. 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. **Note:** Use the 'avc-update-interval' and 'wireless-clients-update-interval' keywords to configure update interval for AVC-related and wireless-clients related information respectively.

wireless-clients-update-interval	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 Usage Guidelines (Data Aggregation and Expiration) on page 1291. 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.
[120|30|300|60|600]	The following keywords are common to all of the above parameters: • 120 – Sets the data-update periodicity as 120 seconds (2 minutes) • 30 – Sets the data-update periodicity as 30 seconds • 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. • 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the 'update-interval' parameter. • 600 – Sets the data-update periodicity as 600 seconds (10 minutes)

```
nsight database statistics max-apps-per-client <1-1000>
```

nsight database statistics	Configures NSight database statistics related parameters
max-apps-per-client	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.
<1-1000>	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>
```

nsight database summary	Configures the NSight database's per-bucket data storage duration
duration <1-24> <1-168> <1-2160> <24-26280>	Configures the duration for which data is stored on a per-bucket basis • <1-24> – Specify the bucket 1 duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours. • <1-168> – Specify the bucket 2 duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours. <1-2160> – Specify the bucket 3 duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours). <24-26280> – Specify the bucket 4 duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year). **Note:** 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 use (rf-domain-config-mode) on page 488. 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 Usage Guidelines (Data Aggregation and Expiration).

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

no on page 1287	Reverts the NSight database related parameters configured to default values

override-wlan

Device Config Commands on page 1265

Configures WLAN's RF Domain level overrides

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

<WLAN>	Specify the WLAN name. Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.
shutdown	Shuts down the WLAN's (identified by the <WLAN> keyword) operations on all mapped radios

SSID <SSID>	Configures the WLAN's Service Set Identifier (SSID) • <SSID> – Specify an SSID ID.
vlan-pool <1-4094> {limit <0-8192>}	Configures a pool of VLANs for the selected WLAN • <1-4094> – Specifies a VLAN pool ID from 1 - 4094. • limit – Optional. Limits the number of users on this VLAN pool <0-8192> – Specify the user limit from 0 - 8192. Note: The VLAN pool configuration overrides the VLAN configuration.
wpa-wpa2-psk <WORD>	Configures the WLAN WPA-WPA2 key or passphrase for the selected WLAN • <WORD> – Specify a WPA-WPA2 key or passphrase.

```
override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]
```

<WLAN>	Specify the WLAN name.
wep128 [key <1-4> hex [0<WORD>| 2 <WORD>]| transmit-key <1-4>	Configures the WEP128 key for this WLAN, and also enables key transmission 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. • key <1-4> hex – Configures a hexadecimal key (clear text or encrypted) and specifies the key's index. • 0 <WORD> – Configures a clear text key. Specify a 4 - 32 character pass key. • 2 <WORD> – Configures an encrypted key. Specify a 4 - 32 character pass key. • transmit-key <1-4> – Enables transmission of key index. Specify the key index. 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.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#override-wlan test vlan-pool 8

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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 94-9B-2C-13-3E-1C 5.8TestAP
 neighbor-info-interval 50
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes RF Domain level WLAN overrides

remove-override

Device Config Commands on page 1265

Removes device overrides in order to enable profile settings to take effect

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`remove-override <PARAMETERS>`

Parameters

```
remove-override <PARAMETERS>
```

remove-override <PARAMETERS>	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 wlans
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)#
```

rsa-key

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`rsa-key ssh <RSA-KEY-NAME>`

Parameters

```
rsa-key ssh <RSA-KEY-NAME>
```

rsa-key ssh <RSA-KEY-NAME>	Assigns RSA key to SSH • <RSA-KEY-NAME> – Specifies the RSA key name. The key should be installed using PKI commands in the enable mode.

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#rsa-key ssh rsa-key1

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes RSA key from service

sensor-server

Device Config Commands on page 1265

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]}
```

sensor-server <1-3>	Sets a numerical index to differentiate this AirDefense sensor server from other servers. A maximum of 3 (three) sensor server resources can be defined.
ip <IP/HOSTNAME>	Configures the AirDefense sensor server's IP address or hostname • <IP/HOSTNAME> – Specify the IP address.
port [443|<1-65535>]	Optional. Configures the port. The options are: • 443 – The default port used by the AirDefense server. This is the default setting. • <1-65535> – Manually sets the port number of the AirDefense server from 1 - 65535

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#sensor-server 1 ip 172.16.10.7

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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 94-9B-2C-13-3E-1C 5.8TestAP
```

```
 neighbor-info-interval 50
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes configured sensor server settings

timezone

Device Config Commands on page 1265

Configures device's timezone

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

`timezone <TIMEZONE>`

Parameters

```
timezone <TIMEZONE>
```

timezone <TIMEZONE>	Configures the device's timezone

Example

```
nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#timezone Etc/UTC

nx9500-6C8809(config-device-94-9B-2C-13-3E-1C)#show context
ap505 94-9B-2C-13-3E-1C
 use profile default-ap505
 use rf-domain default
 hostname TechPubAP505
 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-94-9B-2C-13-3E-1C)#
```

Related Commands

no on page 1287	Removes device's configured timezone

trustpoint (device-config-mode)

Device Config Commands on page 1265

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 1245.

Note
Certificates/trustpoints used in this command should be verifiable as existing on the device.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>
```

trustpoint	Assigns trustpoints to validate various services. The assigned trustpoint is used as the CA for validating the services.
cloud-client	Assigns trustpoint to validate cloud client. The trustpoint should be existing and installed on the device. 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,
cmp-auth-operator	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. Note: When configured, this cmp-auth-operator trustpoint setting overrides the profile-level configuration.
https	Assigns an existing trustpoint to validate HTTPS
radius-ca	Assigns an existing trustpoint to validate client certificates in EAP
radius-ca-ldaps	Assigns an existing trustpoint to validate external LDAP server

radius-server	Assigns an existing trustpoint to validate RADIUS server certificate
radius-server-ldaps	Assigns an existing trustpoint to RADIUS server certificate to validate LDAP server
<TRUSTPOINT-NAME>	The following keyword is common to all of the above parameters: • <TRUSTPOINT-NAME> – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device). **Note:** By default, the system assigns the default-trustpoint to validate the following: https, radius-server, and radius-server-ldaps.

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 1265

Enables chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a service platform

The NX9500 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 NX9500 series service platforms, they can be administrated on behalf of a NX9500 profile by a different model service platform or wireless controller.

Supported in the following platforms:

- Service Platforms — NX7500, NX9500, NX9600

Syntax

```
raid alarm enable
```

Parameters

```
raid alarm enable
```

alarm enable	Enables audible alarm, which is triggered a RAID drives fails. When triggered the alarm can be disabled by executing the raid > silence 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 ge1
  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

no on page 1214	Disables RAID alarm

9 AAA Policy

aaa-policy-commands

This chapter summarizes the AAA *(Authentication, Authorization, and Accounting)* policy commands in the CLI command structure.

An 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 *attribute-value* (AV) 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                    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
--More--
nx9500-6C8809(config-aaa-policy-test)#
```

```
ap505-13403B(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

ap505-13403B(config-aaa-policy-test)#
```

aaa-policy-commands

The following table summarizes the AAA policy configuration mode commands:

Table 39: AAA Policy Configuration Commands

Command	Description
accounting on page 1305	Configures accounting parameters
attribute on page 1310	Configure RADIUS attributes in access and accounting requests
authentication on page 1313	Configures authentication parameters

Table 39: AAA Policy Configuration Commands (continued)

Command	Description
health-check on page 1319	Configures health check parameters
mac-address-format on page 1320	Configures the MAC address format
proxy-attribute on page 1321	Configures the RADIUS server's attribute behavior when proxying through the wireless controller or the RF Domain manager
server-pooling-mode on page 1322	Defines the method for selecting a server from the pool of configured AAA servers
use on page 1323	Defines the AAA command settings
no on page 1323	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <0-63> – Sets the DSCP value from 0 - 63. The default value is 34.
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. • <50-200> – Specify a value from 50 - 200. The default is 100. If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries. If the scaling factor is less than 100, the interval between two consecutive retires reduces with subsequent retries. If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries.

```
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 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 • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server's UDP port (the port used to connect to the accounting server) • <1-65535> – Specify the port number from 1 - 65535. The default value is 1813.

```
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. 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|suffix]	Select one of the following options: • prefix – Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting. • suffix – Matches the suffix of the username (For example, user1@DOMAIN, user2)@DOMAIN)
realm <REALM-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. • <REALM-TEXT> – Specifies the matching text including the delimiter (a delimiter is typically '' or '@')
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 <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 • <1-60> – Specify a value from 1 - 60 seconds. The default is 5 seconds.
{attempts<1-10>}	Optional. Specifies the number of attempts made at transmitting a request before being dropped • <1-10> – Specify a value from 1 - 10. The default is 3.

```
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 on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *accounting-delay-time* 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. 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 *accounting-multi-session-id* 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 *chargeable-user-identity* attribute. This option is disabled by default.

```
attribute cisco-vsa audit-session-id
```

cisco-vsa audit-session-id	Configures the CISCO VSA *(Vendor Specific Attribute)* attribute included in access requests. This feature s disabled by default. 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). • audit-session-id – Includes the audit session ID attribute in access requests The audit session ID is included in access requests when Cisco ISE is configured as an authentication server. **Note:** 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 service on page 1259.

```
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 <100-1500>	Configures Framed-MTU attribute used in access 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. 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. • <100-1500> – Specify the Framed-MTU attribute value from 100 - 1500. The default value is 1400.

```
attribute location-information [include-always|none|server-requested]
```

location-information [include-always| none|server-requested]	Enables support for RFC5580 location information attribute, based on the option selected. The options are: • include-always – Always includes location information in RADIUS authentication and accounting messages • none – Disables sending of location information in RADIUS authentication and accounting messages. This is the default setting. • server-requested – Includes location information in RADIUS authentication and accounting messages only when requested by the server Note: When enabled, location information is exchanged in authentication and accounting messages.

```
attribute nas-ip-address <WORD>
```

nas-ip-address <WORD>	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. • <WORD> – Provide the IPv4 address.

```
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. • <OPERATOR-NAME> – Specify the network operator's name (should not exceed 63 characters in length).

```
attribute service-type [framed|login]
```

service-type [framed|login]	Configures the *service-type (6)* attribute value. This attribute identifies the following: the type of service requested and the type of service to be provided. • framed – Sets *service-type to framed (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. • login – Sets *service-type to login (1)* in the authentication packets. When enabled, the client is connected to the host.

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 on page 1323	Resets values or disables commands

authentication

Configures user authentication parameters

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-10> – Specify a value from 1 - 10. The default is 3.
identity-request-retry- timeout <10-5000>	Configures the interval, in milliseconds, after which an EAP-identity request to the wireless client is retried • <10-5000> – Specify a value from 10 - 5000 milliseconds. The default is 1000 milliseconds.
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) • <1-60> – Specify a value from 1 - 60 seconds. The default is 30 seconds.

retry-timeout-factor <50-200>	Configures the interval between successive EAP retries • <50-200> – Specify a value from 50 - 200. The default is 100. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.
timeout <1-60>	Configures the interval, in seconds, between successive EAP-identity request sent to a wireless client • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.

```
authentication protocol [chap|mschap|mschapv2|pap]
```

protocol [chap|mschap| mschapv2| pap]	Configures one of the following protocols for non-EAP authentication: • chap – Uses CHAP *(Challenge Handshake Authentication Protocol)* • mschap – Uses MS-CHAP *(Microsoft Challenge Handshake Authentication Protocol)* • mschapv2 – Uses MS-CHAP version 2 • pap – Uses PAP *(Password Authentication Protocol)*. This is the default setting.

```
authentication server <1-6> dscp <0-63>
```

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
dscp <0-63>	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. • <0-63> – Specify the value from 0 - 63. The default is 46.

```
authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|
2 <SECRET>|<SECRET>] {port <1-65535>}
```

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
host <IP/HOSTNAME>	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.

secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures the RADIUS authentication server's secret key. This key is used to authenticate with the RADIUS server. • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the RADIUS authentication server's UDP port (this port is used to connect to the RADIUS server) • <1-65535> – Specify a value from 1 - 65535. The default port is 1812.

```
authentication server <1-6> nac
```

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
nac	Enables NAC *(Network Access Control)* on the RADIUS authentication server identified by the <1-6> parameter. 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.).

```
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. • <1-6> – Specifies the RADIUS server index from 1 - 6.
nai-routing	Enables NAI routing. When enabled, AAA servers identify clients using NAI. This option is disabled by default. 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 [prefix|suffix]	Configures the realm-type used for NAI authentication • prefix – Sets the realm prefix. For example, in the realm name 'AC \JohnTalbot', the prefix is 'AC' and the user name 'JohnTalbot'. • 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'.

realm <REALM-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. • <REALM-NAME> – Sets the realm used for authentication. This value is matched against the user name provided for RADIUS authentication. Example: Prefix - AC\JohnTalbot Suffix - JohnTalbot@AC.org
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 *strip* 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. • <1-6> – Specify the RADIUS server index from 1 - 6.
onboard [centralized-controller|controller|self]	Selects the onboard RADIUS server for authentication instead of an external host • centralized-controller – Configures the server on the centralized controller managing the network • controller – Configures the wireless controller, to which the AP is adopted, as the onboard wireless controller • self – Configures the onboard server on the device (AP or wireless controller) where the client is associated as the onboard wireless controller

```
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. • <1-6> – Sets the RADIUS server index between 1 - 6
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 • none – Proxying is not done. The packets are sent directly using the IP address of the device. This is the default setting. • through-centralized-controller – The traffic is proxied through the centralized controller that is configuring and managing the network. • through-controller – The traffic is proxied through the wireless controller configuring this device. • through-mint-host <HOSTNAME/MINT-ID> – The traffic is proxied through a neighboring MiNT device. Provide the device's hostname or MiNT ID. • through-rf-domain-manager – The traffic is proxied through the local RF Domain manager.

```
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. • <1-6> – Specify the RADIUS server index from 1 - 6.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between two consecutive RADIUS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.

```
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 • <1-6> – Specify the RADIUS server index from 1 - 6.
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. • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. In case of no response from the RADIUS authentication server, this option configures he maximum number of attempts made in contacting the server, before retiring the request • <1-10> – Specify a value from 1 -10. The default is 3.

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

no on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
health-check interval <60-86400>
```

Parameters

```
health-check interval <60-86400>
```

interval <60-86400>	Configures an interval (in seconds) after which a down server is checked to see if it is reachable again • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 3600 seconds.

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 on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 AABBCC-DDEEFF
no-delim	Configures the MAC address format as AABBCCDDEEFF (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 • lower – Indicates MAC address is in lower case. For example, aa:bb:cc:dd:ee:ff • upper – Indicates MAC address is in upper case. For example, AA:BB:CC:DD:EE:FF (default setting)
attributes [all|username-password]	Configures RADIUS attributes to which this MAC format is applicable • all – Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id • username-password – Applies only to the username and password fields (default setting)

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 on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 [originator|proxier]	Uses NAS identifier • 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. • proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager.
nas-ip-address [none|proxier]	Uses NAS IP address • none – NAS IP address attribute is not filled • 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.

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 on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1323	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use nac-list <NAC-LIST-NAME>
```

Parameters

```
use nac-list <NAC-LIST-NAME>
```

nac-list <NAC-LIST-NAME>	Associates a NAC list with this AAA policy • <NAC-LIST-NAME> – Specify the NAC list name (should be existing and configured).

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

no on page 1323	Dissociates a NAC list from this AAA policy
nac-list	Creates a NAC list

no

Removes this AAA policy settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

no <PARAMETERS>	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)#
```

10 Auto-Provisioning Policy

auto-provisioning-policy-commands

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 ap505 10 profile default vlan 10
rule #2 adopt ap510 20 profile default vlan 20
rule #3 adopt ap505 30 profile default serial-number
rule #4 adopt ap505 40 p d mac aa bb
```

AP505 L2 adoption, VLAN 10 - will use rule #1

AP505 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 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 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 915.

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 40: Auto Provisioning Policy Configuration Commands

Command	Description
adopt on page 1328	Adds a permit adoption rule
auto-create-rfd-template on page 1333	Enables auto creation of a new RF Domain based on an existing RF Domain template specified using this command
default-adoption on page 1334	Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain
deny on page 1335	Adds a deny adoption rule
evaluate-always on page 1337	Runs this policy every time a device is adopted
redirect on page 1338	Adds a rule redirecting device adoption to a specified controller within the system
upgrade on page 1341	Adds a device upgrade rule to this auto provisioning policy
no on page 1344	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
adopt [anyap|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]

adopt [anyap|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile|rf-domain]

adopt [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

adopt [anyap|ap505|ap510|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|ap505|ap520|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. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
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 AP505 device profile for an AP505. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. 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 Usage Guidelines: Built-in Tokens & Alias on page 1332 for the different types of built in tokens available in the system.

rf-domain <RF-DOMAIN-NAME>	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. 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]'. 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: *test.example_company.com*.
any	Indicates any device. Any device seeking adoption is adopted.

```
adopt [anyap|ap505|ap510|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	Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
precedence <1-10000>	Sets the rule precedence. 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 AP505 device profile for an AP505 . Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. Provide a device profile name (should be existing and configured). Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor'.
rf-domain <RF-DOMAIN-NAME>	Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain. Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]'. Note: 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: *test.example_company.com*.

area <AREA-NAME>	Matches the area of deployment. This option is not applicable to the 'rf-domain' parameter. • <AREA-NAME> – Enter a 64 character maximum deployment area name assigned to this policy. Devices with matching area names are adopted.
cdp-match <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. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are adopted.
dhcp-option <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. • <DHCP-OPTION> – Specify the DHCP option. Devices matching the specified value are adopted.
floor <FLOOR-NAME>	Matches the floor name. This option is not applicable to the 'rf-domain' parameter. • <FLOOR-NAME> – Enter a 32 character maximum deployment floor name assigned to this policy. Devices with matching floor names are adopted.
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. • <FQDN> – Specify the FQDN name. Devices matching the specified value are adopted.
ip [<START-IP> <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. • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <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. • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IPv6 address.

lldp-match <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. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified value are adopted.
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. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Adopts a device if its model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number to match.
serial-number <SERIAL-NUMBER>	Adopts a device if its serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number to match.
vlan <VLAN-ID>	Adopts a device if its VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

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 on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
auto-create-rfd-template <RF-DOMAIN-NAME>
```

Parameters

```
auto-create-rfd-template <RF-DOMAIN-NAME>
```

auto-create-rfd-template <RF-DOMAIN-NAME>	Auto creates a new RF Domain based on an existing RF Domain template • <RF-DOMAIN-NAME> – 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. **Note:** For more information on configuring tokens, see Usage Guidelines: Built-in Tokens & Alias on page 1332.

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 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
deny [anyap|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
deny [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
precedence <1-10000> any
deny [anyap|ap505|ap520|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|aap505|ap510|rfs4000|nx5500|nx75xx|nx9000|vx9000|nx9600]
precedence <1-10000> any
```

deny	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 **Note:** Use the 'anyap' option to auto provision any AP regardless of its model type.
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|ap505|ap510|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	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence. After specifying the rule precedence, specify the match criteria. Devices matching the specified criteria are denied adoption.
cdp-match <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. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are denied adoption.
dhcp-option <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. • <DHCP-OPTION> – Specify the DHCP option value to match. Devices matching the specified value are denied adoption.
fqdn <FQDN>	Matches a substring to the FQDN 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. • <FQDN> – Specify the FQDN. Devices matching the specified value are denied adoption.
ip [<START-IP> <END-IP>| <IP/MASK>]	Denies adoption if a device's IP address matches the specified IPv4 address or is within the specified IP address range • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Denies adoption if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IPv6 address.

lldp-match <LLDP-STRING>	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. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified values are denied adoption.
mac <START-MAC> {<END-MAC>}	Denies adoption if a device's 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. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Denies adoption if a device's model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number to match.
serial-number <SERIAL-NUMBER>	Denies adoption if a device's serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number to match.
vlan <VLAN-ID>	Denies adoption if a device's VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

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

no on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
redirect [anyap|ap505|ap510|rfs4000|nx5500|nx75XX|nx95XX|vx9000|nx96XX]
redirect [anyap|ap505|ap510|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|ap505|ap510|rfs4000||nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any
redirect[anyap|ap505|ap510|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|ap505|ap510|rfs4000||nx5500|nx75XX|nx95XX|vx9000|nx96XX] precedence
<1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any
```

redirect	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 **Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type. **Note:** 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 controller on page 915
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname • ipv6 – Specify the controller's IPv6 address
any	Indicates any device. Any device seeking adoption is redirected.

```
redirect [anyap|ap505|ap510|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	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 **Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type. **Note:** 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 controller on page 915.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.

controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME>|ipv6]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname • ipv6 – Specify the controller's IPv6 address After specifying the rule precedence and the controller, specify the match criteria.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are redirected.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match 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. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are redirected.
fqdn <FQDN>	Configures the FQDN to match 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. • <FQDN> – Specify the FQDN. Devices matching the specified value are redirected.
ip [<START-IP> <END-IP>|<IP/MASK>]	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. • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
level[1|2]	Configures the routing level • level1 – Specifies level 1 as local routing • level2 – Specifies level2 as inter-site routing
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Redirects if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.
lldp-match <LLDP-STRING>	Configures the device location to match, based on LLDP snoop string LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the location. Devices matching the specified string are redirected.

mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are redirected. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are redirected.
pool <1-2>	Configures the controller pool • <1-2> – Configures the pool to which the specified controller belongs to. The default pool value is 1.
serial-nuber <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are redirected.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN ID are redirected.
upgrade	Optional. Upgrades APs before redirecting the device for adoption within the system

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

no on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
upgrade [anyap|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]

upgrade [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> any

upgrade [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> any
```

upgrade	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
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|ap505|ap510|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	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are upgraded.

dhcp-option <DHCP-OPTION>	Configures the DHCP options to match 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. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are upgraded.
fqdn <FQDN>	Configures the FQDN to match. 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. • <FQDN> – Specify the FQDN. Devices matching the specified value are upgraded.
ip [<START-IP> <END-IP>|<IP/MASK>]	Upgrades if a device's IPv4 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Upgrades if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.
lldp-match <LLDP-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. • <LLDP-STRING> – Specify the location. Devices matching the specified string are upgraded.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are upgraded.
serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Device with the specified serial number is upgraded.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.

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

no on page 1344	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
upgrade [anyap|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]

upgrade [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> any

upgrade [anyap|ap505|ap510|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|ap505|ap510|rfs4000|nx5500|nx75xx|nx95xx|vx9000|nx96xx]
precedence <1-10000> any
```

upgrade	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
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|ap505|ap510|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	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: AP505, AP510, RFS4000, NX5500, NX7500, NX9500, NX9600, VX9000 Note: Use the 'anyap' option to auto provision any AP regardless of its model type.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are upgraded.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match 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. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are upgraded.
fqdn <FQDN>	Configures the FQDN to match. 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. • <FQDN> – Specify the FQDN. Devices matching the specified value are upgraded.
ip [<START-IP> <END-IP>|<IP/MASK>]	Upgrades if a device's IPv4 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.

ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Upgrades if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.
lldp-match <LLDP-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. • <LLDP-STRING> – Specify the location. Devices matching the specified string are upgraded.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are upgraded.
serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Device with the specified serial number is upgraded.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.

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

no on page 1344	Removes an upgrade rule from this Auto Provisioning Policy

11 Association-ACL Policy

Association-acl-policy-commands

This chapter summarizes the association *Access Control List* (ACL) 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 41: Association ACL Policy Configuration Commands

Command	Description
deny on page 1349	Specifies a range of MAC addresses denied access to the WLAN
permit on page 1350	Specifies a range of MAC addresses allowed access to the WLAN
no on page 1352	Removes a deny or permit rule from this association ACL policy

Note
For information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Common Commands on page 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <1-1000> – Specify a precedence value from 1 - 1000.

```
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. • <1-1000> – Specify a value from 1 - 1000.

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 on page 1352	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <1-1000> – Specify a value from 1 - 1000.

```
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. • <1-1000> – Specify a value from 1 - 1000.

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 on page 1352	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

12 Access-List Policy

ip-access-list
mac-access-list
ipv6-access-list
ip-snmp-access-list
ex3500-ext-access-list
ex3500-std-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 *Access Control Entries* (ACEs). 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 1356
- ipv6-access-list on page 1400

- mac-access-list on page 1385
- ip-snmp-access-list on page 1412
- ex3500-ext-access-list on page 1414
- ex3500-std-access-list on page 1421

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-ext-access-list on page 1414.
- ex3500-std-access-list on page 1421.
- 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 42: IP-Access-List-Config Commands

Command	Description
deny (ipv4-acl) on page 1356	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).
disable (ipv4-acl) on page 1368	Disables an existing deny or permit rule without removing it from the ACL
insert (ipv4-acl) on page 1371	Inserts a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence
permit (ipv4-acl) on page 1373	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).
no (ipv4-acl) on page 1384	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Applies this deny rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). 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. **Note:** For more information on configuring network-service alias, see alias.
<SOURCE-IP/MASK>	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.

<NETWORK-GROUP-ALIAS-NAME>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). 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).
any	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.
from-vlan <VLAN-ID>	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. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	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. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	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.
any	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.
host <DEST-HOST-IP>	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. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	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.

mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. ICMP packets received from any source are dropped.
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 dropped. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
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 dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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>	Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped.
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 dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<ICMP-TYPE>	Defines the ICMP packet type 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 For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable." Note: 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 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>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. IP packets received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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 dropped.
any	Specifies the destination as any IP address. IP packets addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.

<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	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.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter
<PROTOCOL-NUMBER>	Filters protocols using their IANA *(Internet Assigned Numbers Authority)* protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
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 advertized 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/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-GROUP-ALIAS-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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.
from-vlan <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. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.

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. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<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. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). Note: After specifying the source and destination IP address(es), specify the action taken in case of a match.
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: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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>	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. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.
any	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.
from-vlan <VLAN-ID>	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. • <VLAN-ID> – 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). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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 dropped.
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 dropped.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
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 dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<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 dropped. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.

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 • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP *(Border Gateway Protocol)* protocol port (179) • dns – The designated DNS *(Domain Name System)* protocol port (53) • ftp – The designated FTP *(File Transfer Protocol)* protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP *(Lightweight Directory Access Protocol)* protocol port (389) • nntp – The designated NNTP *(Network News Transfer Protocol)* protocol port (119) • ntp – The designated NTP *(Network Time Protocol)* protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP *(Session Initiation Protocol)* protocol port (5060) • smtp – The designated SMTP *(Simple Mail Transfer Protocol)* protocol port (25) • ssh – The designated SSH *(Secure Shell)* protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP *(Trivial File Transfer Protocol)* protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	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.

rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above:
	• rule-precedence – Assigns a precedence for this deny rule
	  • <1-5000> – Specify a value from 1 - 5000.
	
	  Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
	  • 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).

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

no (ipv4-acl) on page 1384	Removes a specified IP deny access rule
alias on page 172	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. Note: 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 • <PROTOCOL-OPTIONS> – Identify the Internet protocol using the options available.
tcp	Disables a rule applicable to TCP packets only
udp	Disables a rule applicable to UDP packets only Note: 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 • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000>	Specify the rule precedence. The deny or permit rule with the specified precedence is disabled. Note: To enable a disabled rule, enter the rule again without the 'disable' keyword. Note: The **no > disable** 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
 disable deny icmp any any rule-precedence 1
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
 disable 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

no (ipv4-acl) on page 1384	Enables a disabled deny or permit rule
alias on page 172	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
<PARMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see deny. For more information on the permit rule, see permit.
log	After specifying the match criteria, specify the action taken for filtered packets 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>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	Assigns a precedence for this deny/permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

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

alias on page 172	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Applies this permit rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). 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. **Note:** For more information on configuring network-service alias, see alias.
<SOURCE-IP/MASK>	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.
<NETWORK-GROUP-ALIAS-NAME>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). 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).
any	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.
from-vlan <VLAN-ID>	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. • <VLAN-ID> – 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). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	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. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	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.
any	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.
host <DEST-HOST-IP>	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. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.

<NETWORK-GROUP-ALIAS-NAME>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	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.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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
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 forwarded.

log	Logs all permit events matching this dns entry. If a dns-name is matched an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
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. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
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. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
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. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<ICMP-TYPE>	Defines the ICMP packet type 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 For example, an ICMP code 3 indicates "Destination Unreachable", code 1 indicates "Host Unreachable", and code 3 indicates "Port Unreachable." Note: 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 <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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/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-GROUP-ALIAS-NAME>	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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any source IP address. IP packets received from any source are permitted.

from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
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 <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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 Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP 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 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 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 protocols are: RIP and OSPF
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 protocol (number 112) VRRP allows a pool of routers to be advertized 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/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-GROUP-ALIAS-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. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are permitted.
from-vlan <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. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
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 permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<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-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. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<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 permitted. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), 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 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: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

```
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/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-GROUP-ALIAS-NAME>	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. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.
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-ID>	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. • <VLAN-ID> – 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). Note: Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.

<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 • <SOURCE-PORT> – Specify the exact source port.
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. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<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. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
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 • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP protocol port (179) • dns – The designated DNS protocol port (53) • ftp – The designated FTP protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP protocol port (389) • nntp – The designated NNTP protocol port (119) • ntp – The designated NTP protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP protocol port (5060) • smtp – The designated SMTP protocol port (25) • ssh – The designated SSH protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.

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 <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above:
	• rule-precedence – Assigns a precedence for this permit rule
	  • <1-5000> – Specify a value from 1 - 5000.
	
	  Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
	  • 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).

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 (ipv4-acl) on page 1384	Removes a specified IP permit access rule
alias on page 172	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be associated with the deny/permit rule).
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> rule-description <LINE>	Specify the precedence assigned to this deny/permit rule. • rule-description – Optional. Specify the rule description. Note: The system removes the rule from the selected ACL.

```
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 • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be associated with the deny/permit rule).
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> rule-description <LINE>	Specify the precedence assigned to this disabled deny/permit rule. • rule-description – Optional. Specify the rule description. Note: The system removes the disabled rule from the selected ACL.

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)#
```

mac-access-list

The following table summarizes MAC Access list configuration commands:

Table 43: MAC-Access-List-Config Commands

Command	Description
deny (mac-acl) on page 1386	Creates a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.
disable (mac-acl) on page 1389	Disables a MAC deny or permit rule without removing it from the ACL
ex3500 (mac-acl-config-commands) on page 1391	Creates a MAC ACL deny and/or permit rule applicable only to the EX3500 switch

Table 43: MAC-Access-List-Config Commands (continued)

Command	Description
insert (mac-acl) on page 1393	Inserts a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence
permit (mac-acl) on page 1395	Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding.
no (mac-acl) on page 1398	Removes a deny and/or a permit access rule from a MAC ACL

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. 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 • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets received from the specified host are dropped.

<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. 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 • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are dropped.
dot1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp| appletalk| arp|ip|ipv6|ipx|mint| rarp| wisp]	Configures the EtherType value 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: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk ARP payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800) • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse ARP payload (0x8035) • wisp – Indicates the WIPS *(Wireless Internet Service Provider)* payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.

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:
	• rule-precedence – Assigns a precedence for this deny rule
	  • <1-5000> – Specify a value from 1 - 5000.
	
	  Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
	  • 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).

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

no (mac-acl) on page 1398	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 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 • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address 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>	Specifies the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address. • <DEST-MAC-MASK> – Specify the destination MAC address mask.
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: • log – Logs a record, when a packet matches the specified criteria
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 • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63 Note: This option is applicable only to the MAC ACL permit rule.
type [8021q|<1-65535>|aarp| appletalk| arp|ip|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: • rule-precedence – Assigns a precedence for this rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

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

no (mac-acl) on page 1398	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 EX3500 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.

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.

Note
To implement the EX3500 MAC ACL rule, apply the MAC ACL directly to a EX3500 device, or to an EX3500 profile. For more information, see #unique_970.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]	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 EX3500 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.
[all|tagged-eth2| untagged-eth2]	Specifies the packet type • all – Applies this deny/permit rule to all packets • tagged-eth2 – Applies this deny/permit rule only to tagged Ethernet-2 packets • untagged-eth2 – Applies this deny/permit rule only to untagged Ethernet-2 packets After specifying the packet type, configure the source and/or EX3500 MAC addresses to match.
[any| host <SOURCE-MAC>| network <SOURCE-MAC> <SOURCE-MAC-MASK>]	Enter the Source MAC addresses • any – Identifies all EX3500 devices as a source to match • host <SOURCE-MAC> – Identifies a specific EX3500 host as the source to match • <SOURCE-MAC> – Specify the source host's exact MAC address • network <SOURCE-MAC> <SOURCE-MAC-MASK> – Configures a range of MAC addresses as the source to match. Packets received from any of these MAC addresses are dropped. • <SOURCE-MAC> – Specify the source MAC address to match. <SOURCE-MAC-MASK> – Specify the source MAC bit mask. For a deny rule, packets received from EX3500 device(s) matching the specified MAC address(es) are dropped. For a permit rule, packets received from EX3500 device(s) matching the specified MAC address(es) are forwarded.
[any|host <DEST-MAC>| network <DEST-MAC> <DEST-MAC-MASK>]	Enter the Destination MAC addresses • any – Identifies all EX3500 devices as a destination to match • host <SOURCE-MAC> – Identifies a specific EX3500 host as the destination to match • <SOURCE-MAC> – Specify the destination host's exact MAC address • network <SOURCE-MAC> <SOURCE-MAC-MASK> – Configures a range of MAC addresses as the destination to match. Packets addressed to any of these MAC addresses are dropped. • <SOURCE-MAC> – Specify the destination MAC address to match. <SOURCE-MAC-MASK> – Specify the destination MAC bit mask. For a deny rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are dropped. For a permit rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are forwarded.
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. • <0-65535> – Specify the value from 0 - 65535. The default value is 1.
ethertype-mask <0-65535>	Configures the Ethertype mask • <0-65535> – Specify the value from 0 - 65535. The default value is 1.

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. • <TIME-RANGE-NAME> – Specify the time range name. 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). Note: For information on configuring EX3500 time-range, see ex3500.
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) • <1-4094> – Specify the VLAN ID from 1 - 4094.
vlan-mask <1-4095>	Configures the VLAN ID bit mask value • <1-4095> – Specify the VLAN bit mask from 1 - 4095.
rule-precedence <1-128>	Configures a precedence for this EX3500 MAC ACL • <1 - 128> – Specify a value from 1 - 128. ACLs with lower precedence are applied first to packets.

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

no (mac-acl) on page 1398	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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
<PARMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see deny. For more information on the permit rule, see permit.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
mark [8021p <0-7>,dscp <0-63>]	Marks/modifies packets that match the criteria specified here • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63 **Note:** This option is applicable only to the MAC ACL permit rule.
type [8021q|<1-65535>| aarp| appletalk| arp|ip|ipv6|ipx|mint| rarp| wisp]	Configures the EtherType value 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: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk ARP payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the IPv4 payload (0x0800) • ipv6 – Indicates the IPv6 payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse ARP payload (0x8035) • wisp – Indicates the WISP payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.

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: • rule-precedence – Assigns a precedence for this deny/permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. 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 • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets received from the specified host are forwarded.
<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. 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 • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are forwarded.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.

type [8021q|<1-65535>| aarp| appletalk| arp|ip|ipv6|ipx|mint| rarp| wisp]	Configures the EtherType value 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: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk ARP payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the IPv4 payload (0x0800) • ipv6 – Indicates the IPv6 payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse ARP payload (0x8035) • wisp – Indicates the WISP payload (0x8783)
vlan <1-4095>	Configures the VLAN ID • <1-4095> – Specify the VLAN ID from 1 - 4095.
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: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • 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).

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

no (mac-acl) on page 1398	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.
dotp1p <0-7>	Specify the 802.1p priority value from 0 -7.
type [8021q|<1-65535>| aarp| appletalk|arp|ip|ipv6|ipx|mint|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 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 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-description <LINE>}	Specify the precedence assigned to this disabled deny/permit rule. • rule-description – Optional. Specify the rule description. Note: The system removes the disabled rule from the selected ACL.

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
```

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 44: IPv6 Access List Config Mode Commands

Command	Description
deny (ipv6-acl) on page 1400	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).
permit (ipv6-acl) on page 1406	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).
no (ipv6-acl) on page 1411	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|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>)}
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. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
<ICMPv6-TYPE> [eq|range]	Defines the ICMPv6 type field filter • eq – Configures a specific ICMPv6 type. Specify the ICMPv6 type value. • range – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values. Note: ICMPv6 packets with type field value matching the values specified here are dropped.
<ICMPv6-CODE>	Defines the ICMPv6 code field filter • eq – Configures a specific ICMPv6 code. Specify the ICMPv6 code value. • range – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values. Note: ICMPv6 packets with code field value matching the values specified here are dropped.
log	Logs all deny events matching this entry

rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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|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 Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP 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 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.
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 protocols are: RIP and OSPF.
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 protocol (number 112) VRRP allows a pool of routers to be advertized 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. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<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 • <SOURCE-PORT> – Specify the exact source port.
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. • <DEST-HOST-IP> – Specify the destination host's exact IP address.

range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| | bgp|dns|ftp| ftp-data|gropher| https| ldap|nntp|ntp| pop3|sip|smtp| ssh| telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP protocol port (179) • dns – The designated DNS protocol port (53) • ftp – The designated FTP protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP protocol port (389) • nntp – The designated NNTP protocol port (119) • ntp – The designated NTP protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP protocol port (5060) • smtp – The designated SMTP protocol port (25) • ssh – The designated SSH protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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

no (ipv6-acl) on page 1411	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|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>)}
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. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
<ICMPv6-TYPE> [eq|range]	Defines the ICMPv6 type field filter • eq – Configures a specific ICMPv6 type. Specify the ICMPv6 type value. • range – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values. Note: ICMPv6 packets with type field value matching the values specified here are forwarded.
<ICMPv6-CODE>	Defines the ICMPv6 code field filter • eq – Configures a specific ICMPv6 code. Specify the ICMPv6 code value. • range – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values. Note: ICMPv6 packets with code field value matching the values specified here are forwarded.
log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.

log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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 Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP 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 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.
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 protocols are: RIP and OSPF.
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 protocol (number 112) VRRP allows a pool of routers to be advertized 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. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<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. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<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 • <SOURCE-PORT> – Specify the exact source port.
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. • <DEST-HOST-IP> – Specify the destination host's exact IP address.
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| | bgp|dns|ftp| ftp-data|gropher| https| ldap|nntp|ntp| pop3|sip|smtp| ssh| telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP protocol port (179) • dns – The designated DNS protocol port (53) • ftp – The designated FTP protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP protocol port (389) • nntp – The designated NNTP protocol port (119) • ntp – The designated NTP protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP protocol port (5060) • smtp – The designated SMTP protocol port (25) • ssh – The designated SSH protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all permit events matching this entry

rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. Note: Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
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)#ermit 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

no (ipv6-acl) on page 1411	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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.

The following table summarizes SNMP access list configuration commands:

Table 45: SNMP Access List Config Mode Commands

Command	Description
deny (ip-snmp acl) on page 1412	Creates a deny SNMP MIB object traffic rule
permit (ip-snmp acl) on page 1413	Creates a permit SNMP MIB object traffic rule
no (ip-snmp acl) on page 1414	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
deny [<IP/M>|any|host <IP>]
```

Parameters

```
deny [<IP/M>|any|host <IP>]
```

deny [<IP/M>|any|host <IP>]	Configures the match criteria for this deny rule • <IP/M> – Specifies a network address and mask in the A.B.C.D/M format. Packets received from or destined for this network are dropped. • any – Specifies the match criteria as any. Packets received from or destined for any address are dropped. • host <IP> – Identifies a host by its IP address. Packets received from or destined for this host are dropped.

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

no (ip-snmp acl) on page 1414	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
permit [<IP/M>|any|host <IP>]
```

Parameters

```
permit [<IP/M>|any|host <IP>]
```

permit [<IP/M>|any|host <IP>]	Configures the match criteria for this permit rule • <IP/M> – Specifies a network address and mask in the A.B.C.D/M format. Packets received from or destined for this network are forwarded. • any – Specifies the match criteria as any. Packets received from or destined for any address are forwarded. • host <IP> – Identifies a host by its IP address. Packets received from or destined for this host are forwarded.

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

no (ip-snmp acl) on page 1414	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

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 EX3500 (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 46: EX3500 Extended Access List Config Mode Commands

Command	Description
deny (ex3500-ext acl) on page 1415	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).
permit (ex3500-ext acl) on page 1417	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).
no (ex3500-ext acl) on page 1420	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 EX3500 device, or to an EX3500 profile. For more information, see #unique_970.

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 — RFS4000
- Service Platforms — NX5500, NX75000, NX9500, NX9600, VX9000

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 • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
[<DEST-NETWORK-IP/MASK>| any| host <DEST-HOST-IP>]	Specifies the destination as any, host, or network • <DEST-NETWORK-IP/MASK> – Configures a network as the destination. Provide the network's IPv4 address along with the mask. • host <DEST-HOST-IP> – Configures a single device as the destination. Provide the host device's IPv4 address. • any – Specifies that the destination can be any device
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 • <0-63> – Specify a value from 0 - 63. Note: Control flags can be used only in ACLs designed to filter TCP traffic. 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. • URG flag - Marks incoming packet as urgent. • ACK flag - Acknowledges receipt of packet • PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer. • 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. • SYN flag - Establishes the 3-way handshake between two hosts • FIN flag - Tears down the connection established between two hosts via the 3-way SYN process
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>). • <0-65535> – Specify the destination port from 0 - 65535.
destination-port-bitmark <0-65535>	Configures the decimal number representing the protocol destination port bits to match • <0-65535> – Specify the destination port bits from 0 - 65535.
dscp <0-63>	Configures the DSCP priority level • <0-63> – Specify a value from 0 - 63. Note: If specifying DSCP priority, ip-precedence cannot be specified.
ex3500-time-range <TIME-RANGE-NAME>	Applies a periodic or absolute time range to this rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see ex3500 on page 313.

ip-precedence <0-7>	Configures the IP header precedence • <0-7> – Specify a value from 0 - 7.
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>). • <0-65535> – Specify the source port from 0 - 65535.
source-port-bitmark <0-65535>	Configures the decimal number representing the protocol source port bits to match • <0-65535> – Specify the source port bits from 0 - 65535.
rule-precedence <1-128>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence to this deny rule • <1-128> – Specify a value from 1 - 5000. **Note:** 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.

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

no (ex3500-ext acl) on page 1420	Removes a specified deny access rule from this IPv4 EX3500 extended ACL

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 — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
[<DEST-NETWORK-IP/MASK>| any| host <DEST-HOST-IP>]	Specifies the destination as any, host, or network • <DEST-NETWORK-IP/MASK> – Configures a network as the destination. Provide the network's IPv4 address along with the mask. • host <DEST-HOST-IP> – Configures a single device as the destination. Provide the host device's IPv4 address. • any – Specifies that the destination can be any device

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 • <0-63> – Specify a value from 0 - 63. Note: Control flags can be used only in ACLs designed to filter TCP traffic. 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. • URG flag - Marks incoming packet as urgent • ACK flag - Acknowledges receipt of packet • PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer. • 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. • SYN flag - Establishes the 3-way handshake between two hosts • FIN flag - Tears down the connection established between two hosts via the 3-way SYN process
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>). • <0-65535> – Specify the destination port from 0 - 65535.
destination-port-bitmark <0-65535>	Configures the decimal number representing the protocol destination port bits to match • <0-65535> – Specify the destination port bits from 0 - 65535.
dscp <0-63>	Configures the DSCP priority level • <0-63> – Specify a value from 0 - 63. Note: If specifying DSCP priority, ip-precedence cannot be specified.
ex3500-time-range <TIME-RANGE-NAME>	Applies a periodic or absolute time range to this rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see ex3500 on page 313.
ip-precedence <0-7>	Configures the IP header precedence • <0-7> – Specify a value from 0 - 7.
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>). • <0-65535> – Specify the source port from 0 - 65535.

source-port-bitmark <0-65535>	Configures the decimal number representing the protocol source port bits to match • <0-65535> – Specify the source port bits from 0 - 65535.
rule-precedence <1-128>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence to this permit rule • <1-128> – Specify a value from 1 - 5000. **Note:** 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.

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

no (ex3500-ext acl) on page 1420	Removes a specified permit access rule from this IPv4 EX3500 extended ACL

no (ex3500-ext acl)

Removes a deny or permit access rule from this IPv4 EX3500 extended ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

no <PARAMETERS>	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 47: EX3500-Standard-Access-List-Config Commands

Command	Description
deny (ex3500-std acl) on page 1422	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.
permit (ex3500-std acl) on page 1423	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.
no (ex3500-std acl) on page 1424	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 EX3500 device, or to an EX3500 profile. For more information, see #unique_970.

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 — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]	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. • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
ex3500-time-range <TIME-RANGE-NAME>	Optional. Applies a periodic or absolute time range to this deny rule • <TIME-RANGE-NAME> – 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 ex3500 on page 313.

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

no (ex3500-std acl) on page 1424	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 — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}
```

permit [<SOURCE-NETWORK-IP/MASK>| any| host <SOURCE-HOST-IP>]	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. • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
ex3500-time-range <TIME-RANGE-NAME>	Optional. Applies a periodic or absolute time range to this permit rule • <TIME-RANGE-NAME> – 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 ex3500 on page 313 .

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

no (ex3500-std acl) on page 1424	Removes a specified permit access rule from this IPv4 EX3500 standard ACL

no (ex3500-std acl)

Removes a deny or permit access rule from this IPv4 EX3500 standard ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [deny|permit] [<SOURCE-IP/MASK>|any|host <IP>]
{ex3500-time-range <TIME-RANGE-NAME>}
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes a deny or permit access rule based on the parameters passed

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)#
```

13 DHCP-Server Policy

dhcp-server-policy commands
dhcpv6-server-policy commands

This chapter summarizes *Dynamic Host Control Protocol* (DHCP) 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 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 1426.
- dhcpv6-server-policy commands on page 1469.

dhcp-server-policy commands

The following table summarizes the DHCP server policy configuration mode commands:

Table 48: DHCP-Server-Policy Config Mode Commands

Command	Description
bootp (dhcpv4-server-policy-config) on page 1427	Configures a *Bootstrap Protocol* (BOOTP) specific configuration
dhcp-class (dhcpv4-server-policy-config) on page 1428	Configures a DHCP server class
dhcp-pool (dhcpv4-server-policy-config) on page 1431	Configures a DHCP server address pool
dhcp-server (dhcpv4-server-policy-config) on page 1467	Configures DHCP server options

Table 48: DHCP-Server-Policy Config Mode Commands (continued)

Command	Description
option (dhcpv4-server-policy-config) on page 1466	Defines the DHCP option used in DHCP pools
ping (dhcpv4-server-policy-config) on page 1466	Specifies ping parameters used by a DHCP server
no (dhcpv4-server-policy-config) on page 1469	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 616.

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. *Bootstrap Protocol* (BOOTP) 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
bootp ignore
```

Parameters

```
bootp ignore
```

bootp ignore	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 1469	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dhcp-class <DHCP-CLASS-NAME>
```

Parameters

```
dhcp-class <DHCP-CLASS-NAME>
```

<DHCP-CLASS-NAME>	Creates a DHCP user class • <DHCP-CLASS-NAME> – 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.

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 49: DHCP-User-Class Config Mode Commands

Command	Description
multiple-user-class (dhcpv4-class-config) on page 1429	Enables or disables multiple user class option for this DHCP user class policy
option (dhcpv4-class-config) on page 1430	Configures DHCP user class options for this DHCP user class policy
no (dhcpv4-class-config) on page 1430	Removes this DHCL class settings
no (dhcpv4-server-policy-config) on page 1469	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv4-class-config) on page 1430	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
option user-class <VALUE>
```

Parameters

```
option user-class <VALUE>
```

user-class <VALUE>	Configures DHCP user class options • <VALUE> – Specify the DHCP user class option's ASCII value.

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

no (dhcpv4-class-config) on page 1430	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dhcp-pool <POOL-NAME>
```

Parameters

```
dhcp-pool <POOL-NAME>
```

<POOL-NAME>	Creates a DHCP server address pool • <POOL-NAME> – 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.

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 50: DHCP-User-Pool Config Mode Commands

address (dhcpv4-pool-config) on page 1433	Specifies a range of addresses for a DHCP address pool
bootfile (dhcpv4-pool-config) on page 1434	Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.
ddns (dhcpv4-pool-config) on page 1435	Configures dynamic DNS parameters
default-router (dhcpv4-pool-config) on page 1437	Configures a default router or gateway IP address for the network pool

Table 50: DHCP-User-Pool Config Mode Commands (continued)

dns-server (dhcpv4-pool-config) on page 1438	Sets a DNS server's IP address available to all DHCP clients connected to the DHCP pool
domain-name (dhcpv4-pool-config) on page 1440	Sets the domain name for the network pool
excluded-address (dhcpv4-pool-config) on page 1440	Prevents a DHCP server from assigning certain addresses to the DHCP pool
lease (dhcpv4-pool-config) on page 1442	Sets a valid lease for the IP address used by DHCP clients in the DHCP pool
netbios-name-server (dhcpv4-pool-config) on page 1443	Configures a NetBIOS (WINS) name server's IP address
netbios-node-type (dhcpv4-pool-config) on page 1444	Defines the NetBIOS node type
network (dhcpv4-pool-config) on page 1445	Configures the network on which the DHCP server is deployed
next-server (dhcpv4-pool-config) on page 1446	Configures the next server in the boot process
option (dhcpv4-pool-config) on page 1446	Configures RAW DHCP options
respond-via-unicast (dhcpv4-pool-config) on page 1447	Sends a DHCP offer and DHCP Ack as unicast messages
static-route (dhcpv4-pool-config) on page 1448	Configures a static route for a DHCP pool
update (dhcpv4-pool-config) on page 1449	Controls the usage of the DDNS service
static-binding (dhcpv4-pool-config) on page 1450	Configures static address bindings
no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. Note: 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 alias on page 172 .
range [<START-IP>| <START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]	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: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range Note: The host aliases should be existing and configured.
class <DHCP-CLASS-NAME>	Optional. Applies additional DHCP options, or a modified set of options to those available to wireless clients. For more information, see dhcp-class (dhcpv4-server-policy-config) on page 1428. • <DHCP-CLASS-NAME> – Sets the DHCP class (should be existing and configured>

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

no (dhcpv4-pool-static-binding) on page 1461	Removes the DHCP pool's configured IP addresses
dhcp-class (dhcpv4-server-policy-config) on page 1428	Creates and configures the DHCP class parameters
alias on page 172	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 1427.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1462	Resets the boot image path for the BOOTP clients
bootp (dhcpv4-server-policy-config) on page 1427	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <DDNS-DOMAIN-NAME>	Sets the domain name used for DNS updates 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: • <IP> – Specifies the primary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DDNS server's IP address. The host alias should be existing and configured. Note: 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 alias on page 172.
{<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: • <IP> – Specifies the secondary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the secondary DDNS server's IP address. The host alias should be existing and configured.

```
ddns ttl <1-864000>
```

ttl <1-864000>	Configures the TTL *(Time To Live)* value for DDNS updates • <1-86400> – Specify a value from 1- 864000 seconds.

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address. The host alias should be existing and configured.
{<IP1>|<HOST-ALIAS- NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – 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. Note: 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 alias on page 172. Note: A maximum of 8 default routers can be configured..

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]	Configures the primary DNS server, using one of the following options:
	• <IP> – Specifies the primary DNS server's IP address
	• <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address
	
	Note: A maximum of 8 DNS server's can be configured.
	
	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:
	`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`
	Note, the above example shows the OpenDNS server as being 208.67.2202.220. The alternative IP address 208.67.222.222 can also be used.
	For more information on the entire configuration that needs to be done to integrate WiNG access point, controllers, and service platform with OpenDNS , see opendns on page 91.

{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – 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. **Note:** 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 alias on page 172.

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 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	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. Note: 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 alias on page 172.

```
excluded-address [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]
```

range [<START-IP>| <START-HOST-ALIAS- NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	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: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range The host aliases should be existing and configured.

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 Note: 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 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – 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. Note: 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 alias on page 172.

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • 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. • 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.

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 1462	Removes the NetBIOS node type settings

network (dhcpv4-pool-config)

Configures the DHCP server's network settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

Parameters

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

<IP/M>	Configures the network number and mask (for example, 192.168.13.0/24)
<NETWORK-ALIAS-NAME>	Configures a network alias to identify the network number and mask • <NETWORK-ALIAS-NAME> – Specify the network alias name. It should be existing and configured. Note: A network alias defines a single network address. 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. For more information, see alias on page 172.

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. Note: 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 alias on page 172.

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1462	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1462	Removes static route settings

update (dhcpv4-pool-config)

Controls the use of the DDNS service

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
update dns {override}
```

Parameters

```
update dns {override}
```

dns {override}	Configures DDNS parameters • override – Optional. Enables DDNS updates on an onboard DHCP server

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

no on page 1462	Removes dynamic DNS service control

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

Parameters

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

client-identifier <CLIENT>	Enables a static binding configuration for a client based on its client identifier (as provided by DHCP option 61 and its key value) • <CLIENT> – Specify the client identifier (DHCP option 61).
hardware-address <MAC>	Enables a static binding configuration for a client based on its MAC address • <MAC> – Specify the MAC address of the client.

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 51: DHCPv4-User-Pool Static-Binding Config Mode Commands

Command	Description
bootfile (dhcpv4-pool-static-binding) on page 1452	Assigns a Bootfile name for the DHCP configuration on the network pool
client-name (dhcpv4-pool-static-binding) on page 1453	Configures a client name
default-router (dhcpv4-pool-static-binding) on page 1453	Configures default router or gateway IP address
dns-server (dhcpv4-pool-static-binding) on page 1454	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool
domain-name (dhcpv4-pool-static-binding) on page 1455	Sets the network pool's domain name
ip-address (dhcpv4-pool-static-binding) on page 1456	Configures a host's fixed IP address
netbios-name-server (dhcpv4-pool-static-binding) on page 1456	Configures a NetBIOS (WINS) name server IP address
netbios-node-type (dhcpv4-pool-static-binding) on page 1457	Defines the NetBIOS node type
next-server (dhcpv4-pool-static-binding) on page 1458	Specifies the next server used in the boot process
option (dhcpv4-pool-static-binding) on page 1459	Configures raw DHCP options
respond-via-unicast (dhcpv4-pool-static-binding) on page 1460	Sends a DHCP offer and DHCP Ack as unicast messages
static-route (dhcpv4-pool-static-binding) on page 1460	Adds static routes installed on DHCP clients
no (dhcpv4-pool-static-binding) on page 1461	Negates or reverts to default this DHCP Pool's static binding settings

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 1427.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

bootp (dhcpv4-server-policy-config) on page 1427	Configures BOOTP protocol parameters
no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address
{<IP1>|<HOST-ALIAS- NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – 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. Note: 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 alias on page 172. Note: A maximum of 8 default routers can be configured.

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

no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]	• Configures the primary DNS server, using one of the following options: • <IP> – Specifies the primary DNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – 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. **Note:** 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 alias on page 172.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

<IP>	Configures a fixed IP address (in dotted decimal format) of the client using this host pool
<HOST-ALIAS-NAME>	Configures a host alias identifying the fixed IP address of the client using this host pool Note: 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 alias on page 172.

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 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS- NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – 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. Note: 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 alias on page 172.

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

no (dhcpv4-pool-static-binding) on page 1461	Resets values or disables DHCP pool static binding settings

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
netbios-node-type [b-node|h-mode|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 • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • 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. • 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.

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

no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. Note: 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 alias on page 172.

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

no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv4-pool-static-binding) on page 1461	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

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>]	Removes a range of IP addresses and host aliases associated with this DHCP pool's address list.
	• <START-IP> – Specify the first IP address in the range.
	• <START-HOST-ALIAS-NAME> – Specify the host alias, mapped to the first IP address in the range.
	  • <END-IP> – Specify the last IP address in the range.
	  • <END-HOST-ALIAS-NAME> – Specify the host alias, mapped to the last IP address in the range.
	Note: The specified IP addresses and host aliases are removed from the DHCP pool's address list.

```
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>	Removes an excluded IP address from the list of addresses that cannot be issued by the DHCP server • <IP> – Specify the IP address.
<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>]	Removes a range of IP addresses and host aliases associated with this DHCP pool's excluded address list. <START-IP> – Specify the first IP address in the range. • <START-HOST-ALIAS-NAME> – Specify the host alias, mapped to the first IP address in the range. • <END-IP> – Specify the last IP address in the range. • <END-HOST-ALIAS-NAME> – Specify the host alias, mapped to the last IP address in the range. • Note: The specified IP addresses and host aliases are removed from the DHCP pool's excluded address list

```
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 • <CLIENT-IDENTIFIER> – Specify the client identifier.

```
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 • <MAC> – Specify the hardware MAC address.

```
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	• Optional. Removes DDNS updates from an onboard DHCP server

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

address	Configures the DHCP server's IP address pool
bootfile	Configures the BOOTP boot file path
ddns	Configures DDNS for use with this DHCP pool
default-router	Configures default routers for this DHCP pool
dns-server	Configures default DNS servers for this DHCP pool
domain-name	Configures the DDNS domain name for this DHCP pool
excluded-address	Configures IP addresses assigned as static addresses
lease	Configures the DHCP lease settings
netbios-name-server	Configures the NetBIOS name server

netbios-node-type	Configures the NetBIOS node type
network	Configures the DHCP server's network settings
next-server	Configures the next server in the BOOTP boot process
option	Configures the DHCP option
respond-via-unicast	Configures how a DHCP request and ACK are sent
static-binding	Configure static binding information
static-route	Configures static routes installed on DHCP clients
update	Controls DDNS service usage

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv4-server-policy-config) on page 1469	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv4-server-policy-config) on page 1469	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 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • 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. • 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. • 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.

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

no (dhcpv4-server-policy-config) on page 1469	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 52: DHCPv6-Server-Policy Config Mode Commands

Command	Description
dhcpv6-pool (dhcpv6-server-policy-config) on page 1470	Creates a DHCPv6 pool and enters its configuration mode
restrict-vendor-options (dhcpv6-server-policy-config) on page 1478	Configures this DHCPv6 server policy's DHCP option settings, such as enterprise (vendor ID)
server-preference (dhcpv6-server-policy-config) on page 1479	Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy
option (dhcpv6-server-policy-config) on page 1477	Configures this DHCP server's preference value. This value is sent in DHCP server replies to the IPv6 client.
no (dhcpv6-server-policy-config) on page 1479t	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dhcpv6-pool <DHPCv6-POOL-NAME>
```

Parameters

```
dhcpv6-pool <DHCPv6-POOL-NAME>
```

<DHCPv6-POOL-NAME>	Creates a DHCPv6 server address pool • <POOL-NAME> – 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.

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

dns-server (dhcpv6-pool-config) on page 1472	Configures this DHCPv6 pool's DNS server
domain-name (dhcpv6-pool-config) on page 1472	Configures this DHCPv6 pool's domain name
network (dhcpv6-pool-config) on page 1473	Configures this DHCPv6 pool's network
option (dhcpv6-pool-config) on page 1474	Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.

refresh-time (dhcpv6-pool-config) on page 1475	Configures this DHCPv6 pool's refresh time in seconds
sip (dhcpv6-pool-config) on page 1475	Configures this DHCPv6 pool's Session Initiation Protocol (SIP) server setting
no (dhcpv6-pool-config) on page 1476	Negates or reverts this DHCPv6 pool's settings
no (dhcpv6-server-policy-config) on page 1479 (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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dns-server <IPv6> {<SECONDARY-IPv6>}
```

Parameters

```
dns-server <IPv6> {<SECONDARY-IPv6>}
```

<IPv6>	Configures the primary DNS server's IPv6 address • <IPv6> – Specify the DNS server's IPv6 address (the server associated with this DHCP pool).
<SECONDARY-IPv6>	Configures the secondary DNS server's IPv6 address • <SECONDARY-IPv6> – Specify the secondary DNS server's IPv6 address (the server associated with this DHCP pool).

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 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv6-pool-config) on page 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (dhcpv6-pool-config) on page 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

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

no (dhcpv6-pool-config) on page 1476	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [dns-server|domain-name|network|option|refresh-time|sip]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <0-254> – Specify a value from 0 -254. The system allows only one code, of the same value, for each DHCP option used in each DHCPv6 server policy.
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. • <1-4294967295> – Specifies the enterprise (vendor) ID. Specify a value from 1 - 4294967295. The option code (1) is reserved for subnet-mask and cannot be used. Each vendor should have a unique vendor ID used by the DHCP server to issue vendor-specific DHCP options.

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

no (dhcpv6-server-policy-config) on page 1479	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 DHCPServerOption1 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

no (dhcpv6-server-policy-config) on page 1479	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
server-preference <0-255>
```

Parameters

```
server-preference <0-255>one
```

server-preference <0-255>	Configures this DHCP server's preference value • <0-255> – Specify a value from 0 - 255.

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

no (dhcpv6-server-policy-config) on page 1479	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

14 Firewall Policy

firewall-policy-commands

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 53: Firewall-Policy Config Mode Commands

Command	Description
acl-logging on page 1483	Enables logging on flow creating traffic
alg on page 1483	Enables an algorithm
clamp on page 1484	Sets a clamp value to limit TCP MSS to inner path-MTU for tunneled packets
dhcp-offer-convert on page 1485	Enables the conversion of broadcast DHCP offers to unicast
dns-snoop on page 1486	Sets the timeout value for DNS entries
firewall on page 1486	Configures the wireless firewall
flow on page 1487	Defines a session flow timeout
ip on page 1489	Configures IP components on this firewall policy
ip-mac on page 1496	Defines an action based on IP-MAC table
ipv6 on page 1498	Configures IPv6 components on this firewall policy
ipv6-mac on page 1502	Defines an action based on IPv6-MAC table
logging on page 1503	Enables enhanced firewall logging
proxy-arp on page 1505	Enables the generation of ARP responses on behalf of another device
proxy-nd on page 1505	Enables the generation of ND responses (for IPv6) on behalf of another device
stateful-packet-inspection-12 on page 1506	Enables stateful packets-inspection in layer 2 firewall
storm-control on page 1506	Defines storm control and logging settings
virtual-defragmentation on page 1508	Enables virtual defragmentation of IPv4 packets
no on page 1510	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **DNS**, **Facetime**, **FTP**, **PPTP**, **SCCP**, **SIP**, and **TFTP**.
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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
dns-snoop entry-timeout <30-86400>
```

Parameters

```
dns-snoop entry-timeout <30-86400>
```

entry-timeout <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

no on page 1510	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 ICPM, 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ip [dos|tcp]
ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|
ip-ttl-zero|ipspoof|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 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 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	Optional. Detects Chargen attacks 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. 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.
fraggle	Optional. Detects Fraggle DoS attacks 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.
ftp-bounce	Optional. Detects FTP bounce attacks 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 an invalid protocol number 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.
ip-ttl-zero	Optional. Enables a check for the TCP/IP TTL field having a value of zero (0) 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.
ipsproof	Optional. Enables a check for the IP spoofing DoS attack IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.
land	Optional. Detects LAND DoS attacks 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-advt	Optional. Detects router-advertisement attacks 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).
router-solicit	Optional. Detects router solicitation attacks 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.") 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.
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. Detects TCP FIN scan attacks 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 *Finish* (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. 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.

tcp-intercept	Optional. Prevents TCP intercept attacks by using TCP SYN cookies A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. 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. 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. 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.
tcp-null-scan	Optional. Detects TCP NULL scan attacks 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. 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.
tcp-post-syn	Optional. Detects TCP post SYN DoS attacks 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.
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. 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.
broacast-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-advt	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-icpm- 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <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 • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

```
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: • one – Routing Type 1(Nimrod routing). This option is disabled by default. • two – Routing Type 2(Mobile IP). This option is disabled by default.
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. 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: • <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 • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

```
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: • End point identification option (disabled by default) • Network service access point address option (disabled by default) • Router alert option (disabled by default) • Home address option in destination option extension header (enabled by default) • Pad1 and PadN options validating (enabled by default) All of these are optional parameters. If no option is specified, the system enables checks as per the default values.
drop-only	This parameter is common to all of the above keywords. 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	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <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 • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

```
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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • <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 • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

```
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	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <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 • notifications – 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)#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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
stateful-packet-inspection-l2
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-fw-policy-testFW)#stateful-packet-inspection-l2
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-1000000> – Sets the number of packets received per second
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 • <WLAN-NAME> – Sets the WLAN ID for the storm control configuration

```
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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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) • <1-16384> – Sets a value from 1 - 16384. The default is 8.
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) • <2-8129> – Sets a value from 2 - 8129. The default is 140.
minimum-first- fragment- length <8-1500>	Optional. Defines the minimum length required for the first fragment (applicable to IPv4 and IPV6 packets) • <8-1500> – Sets a value from 8 - 1500 bytes. The default is 8 bytes.
timeout <1-60>	Optional. Configures a virtual de-fragmentation timeout, in seconds, applicable to both IPv4 and IPv6 packets • <1-60> – Specify a value from 1 - 60 seconds. The default is 1 second.

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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-advt|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)#
```

15 MiNT Policy

mint-policy-commands

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 54: MiNT-Policy Config Mode Commands

Command	Description
level on page 1513	Configures the MiNT routing level
lsp on page 1514	Enables adding of checksum to LSP messages forwarded across MiNT links
mtu on page 1514	Configures the global MiNT MTU
router on page 1515	Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)

Table 54: MiNT-Policy Config Mode Commands (continued)

Command	Description
udp on page 1516	Configures the MiNT UDP/IP encapsulation parameters
no 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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
level 2 area-id <1-16777215>
```

Parameters

```
level 2 area-id <1-16777215>
```

level 2	Configures level 2 inter-site MiNT routing
area-id <1-16777215>	Configures the routing area identifier • <1-1677215> – Specify a value from 1 - 16777215. 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.

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mtu <900-1500>
```

Parameters

```
mtu <900-1500>
```

mtu <900-1500>	Specifies the maximum packet size from 900 - 1500 bytes The maximum packet size specified is rounded down to a value using the following formula: 4 + a multiple of 8. 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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. **Note:** 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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
udp port <2-65534>
```

Parameters

```
udp port <2-65534>
```

port <2-65534>	Configures default UDP port used for MiNT control packet encapsulation • <2-65534> – 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.

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

no 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

16 Management Policy

management-policy-commands

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 55: Management-Policy Config Mode Commands

Command	Description
aaa-login on page 1520	Configures login authentication settings
allowed-locations on page 1522	Configures a user-role based access control to RF Domains and locations
banner on page 1524	Configures the MOTD *(message of the day)* text
ftp on page 1525	Enables FTP on this management policy
http on page 1526	Enables HTTP on this management policy
https on page 1527	Enables HTTPS on this management policy
idle-session-timeout on page 1528	Sets the interval after which an idle session is terminated

Table 55: Management-Policy Config Mode Commands (continued)

Command	Description
ipv6 (management-policy) on page 1529	Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively
password-entry on page 1531	Configures user-account lockout and unlock parameters
privilege-mode-password on page 1532	Configures the CLI's privilege mode access password
rest-server (management-policy) on page 1536	Enables the REST *(Representational State Transfer)* server to facilitate device on-boarding
restrict-access on page 1537	Restricts management access to a set of hosts or subnets
snmp-server on page 1539	Sets the SNMP server settings on this management policy
ssh on page 1544	Enables SSH on this management policy
t5 (management-policy) on page 1545	Configures SNMP server settings for T5 devices on this management policy. This command is available only RFS 4000, NX 95XX and NX 96XX platforms.
telnet on page 1547	Enables Telnet on this management policy
user (management-policy) on page 1548	Creates a new user account
service on page 1554	Invokes service commands to troubleshoot or debug (config-if) instance configurations
no (management-policy) on page 1555	Removes or resets this management policy's settings

Note
For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see Common Commands on page 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 **Note:** 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. • <AAA-POLICY-NAME> – Specify the AAA policy name (should be existing and configured). **Note:** For more information on configuring AAA policy, see AAA Policy on page 1303.

```
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 • <AAA-TACACS-POLICY-NAME> – Specify the TACACS policy name (should be existing and configured). **Note:** For more information on configuring AAA TACACS policy, see AAA-TACACS Policy on page 1763.

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

no	Removes the TACACS server policy settings

allowed-locations

Configures an allowed-locations tag and associates locations (RF Domains/sites/tree-node paths) with the tag. In the management policy, create an allowed-locations tag and associate it with a user to restrict the user's access to the locations associated with the tag.

Note

The allowed-locations tag is ONLY applicable to the WiNG 'device-provisioning-admin' user. By applying the allowed-locations tag, the device provisioning user will only be able to provision devices that fall within his/her purview of responsibility.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 single or multiple locations (RF Domains/sites/tree-node paths) with the tag • <WORD> – Provide a location tag name not exceeding 32 characters in length. The name should be user-friendly and should easily identify the associated locations.
locations [NONE|ALL| <LIST-OF-LOCATIONS>]	Associates locations with the above created location tag • NONE – Use this option to specify that this allowed-locations tag has no associated locations. Users associated with this location tag will have access to *none* of the RF Domains/sites/tree-node paths defined within your managed network. • ALL – Use this option to specify that this allowed-locations tag is associated with all locations within your managed network. Users associated with this location tag will have access to all RF Domains/ sites/tree-node paths defined within your managed network. • <LIST-OF-LOCATIONS> – Use this option to associate a list of locations with this allowed-locations tag. You can associate a single RF Domain or multiple RF Domains (for example, test1 test2 test3). You can also define the location as a single tree-node path (for example, /US/CA/SJ/Site-1) or multiple tree-node paths (for example, /US/CA/SJ/ SJSite-1 /US/CA/LA/LACampus-1).Users associated with this location tag will have access only to RF Domains or sites associated with this tag. Note: After configuring the allowed locations tag, use the `user` command to associate this tag with a device-provisioning-admin user. Once associated, the device-provisioning-admin user will have access only to the RF Domains/sites associated with this tag.

Example

```
nx9500-6C8809(config-management-policy-test)#allowed-locations TechPubs
locations /US/CA/SJ/TechPubs
nx9500-6C8809(config-management-policy-test)#allowed-locations TEST locations NONE
nx9500-6C8809(config-management-policy-test)#show context
management-policy test
 telnet
 no http server
 https server
 ssh
 user admin password 1 superuser role superuser access all
 allowed-location TEST locations NONE
 allowed-location TechPubs locations /US/CA/SJ/TechPubs
nx9500-6C8809(config-management-policy-test)#
```

An allowed-locations tag can be associated with multiple RF Domains, as shown in the following example:

```
nx9500-6C8809(config-management-policy-test1)#show context
management-policy test1
 telnet
 no http server
 https server
 ssh
 user admin1 password 1 superuser1 role superuser access all
 user dev-admin1 password 1 dev-admin1 role device-provisioning-admin access all allowed-
locations SanJose                                                              e
 allowed-location TEST locations None
```

```
 allowed-location TechPubs locations /US/CA/SJ/TechPubs
 allowed-location SanJose locations test1 test2 test3
nx9500-6C8809(config-management-policy-test1)#
```

An allowed-locations tag can be associated with multiple tree-node paths as shown in the following example:

```
nx9500-6C8809(config-management-policy-test2)#show context
management-policy test2
 telnet
 no http server
 https server
 ssh
 user admin2 password 1 superuser2 role superuser access all
 user dev-admin2 password 1 dev-admin2 role device-provisioning-admin access allowed-
locations California
 allowed-location California locations /US/CA/SJ/SJEngineering /US/CA/LA/LAEngineering
nx9500-6C8809(config-management-policy-test2)#
```

Note
For more information on configuring tree-node on an RF Domain, refer to tree-node on page 487.

Related Commands

no	Removes an 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
banner motd <LINE>
```

Parameters

```
banner motd <LINE>
```

motd <LINE>	Sets the motd banner • <LINE> – Enter the message string. The message string should not exceed 255 characters.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <ENCRYPTED-PASSWORD> – Specify the password. The password should not exceed 63 characters in length.
<PASSWORD>	Configures a clear text password

```
ftp {rootdir <DIR>}
```

ftp rootdir <DIR>	Optional. Configures the root directory for FTP logins • <DIR> – Specify the root directory path. By default the root directory is set to flash:/

```
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. • <USERNAME> – Specify the username. The username should not exceed 32 characters in length.
password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]	Configures an encrypted password • 1 <ENCRYPTED-PASSWORD> – Specifies an encrypted password (use this option if copy pasting from another device). The password should not exceed 63 characters in length. • <PASSWORD> - Configures a clear text password
rootdir <DIR>	After specifying the password, configure the FTP root directory. • rootdir <DIR> – Configures the root directory for FTP logins. Specify the root directory path.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
[server|sslv3|use-secure-ciphers-only]
```

Parameters

```
[server|sslv3|use-secure-ciphers-only]
```

https server	Configures secure HTTP related parameters on this management policy
server	Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication. This option is enabled by default.
sslv3	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.
use-secure-ciphers-only	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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
idle-session-timeout <1-4320>
```

Parameters

```
idle-session-timeout <1-4320>
```

<1-4320>	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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <IPv6> – Specify the host's IPv6 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host is denied access)

```
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 • <IPv6> – Specify the host's IPv6 address.
subnet <IPv6-PREFIX>	Optional. Restricts access to the host on a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

```
ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>
```

ipv6-access-list <IPv6-ACCESS-LIST-NAME>	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. • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 ACL name.

```
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
```

subnet <IPv6-PREFIX>	Restricts management access to a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

```
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}
```

subnet <IPv6-PREFIX>	Restricts management access to a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
host <IPv6>	Optional. Restricts management access to a specific host within the specified subnet • <IPv6> – Specify the host's IPv6 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

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>	Configures user-role based account lockout criteria • role – Select the user-role. The options are: • device-provisioning-admin • helpdesk • monitor • network-admin • security-admin • system-admin • vendor-admin • web-user-admin max-fail <1-100> – Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 - 100. lockout-time <<0-600> – 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. 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. Note: 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 event on page 352.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

Parameters

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

privilege-mode-password	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.
<PASSWORD/HASHED-STRING-ALIAS-NAME>	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. Note: 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. Note: For more information on configuring a hashed-string alias, see alias.

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
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
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

no (management-policy) on page 1555	Removes the configured CLI privilege mode access password

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

Parameters

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

privilege-mode-password	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. •
<PASSWORD/HASHED-STRING-ALIAS-NAME>	<PASSWORD/HASHED-STRING-ALIAS-NAME> – 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. Note: 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. Note: For more information on configuring a hashed-string alias, see alias.

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
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
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

no	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 1548.

The REST server is enabled by default.

Supported in the following platforms:

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

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <IP> – Specify the host's IPv4 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests. • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

```
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 • <IP> – Specify the host's IPv4 address.
subnet <IP/M>	Optional. Restricts access on a specified subnet • <IP/M> – Sets the subnet in the A.B.C.D/M format
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

```
restrict-access ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list	Uses an IPv4 access list to filter access requests 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 • <IP/M> – Specify the subnet in the A.B.C.D/M format
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when access request received from a host within the specified subnet is denied)

```
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

subnet <IP/M>	Restricts management access to a specified subnet • <IP/M> – Specify the subnet in the A.B.C.D/M format
host <IP>	Uses the host IP address as a second filter • <IP> – Specify the host's IPv4 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when access request received from a host within the specified subnet is denied)

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.

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 <WORD>| 2 <WORD>| <WORD>]	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. • 0 <WORD> – Sets a clear text SNMP community string • 2 <WORD> – Sets an encrypted SNMP community string • <WORD> – Sets the SNMP community string
[ro|rw]	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 • ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information) • rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)
ip-snmp-access-list <IP-SNMP-ACL-NAME>	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.

```
snmp-server enable traps
```

enable traps	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. 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. 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. SNMP trap notifications exist for most controller operations, but not all are necessary for day-to-day operation.

```
snmp-server host <IP> [v1|v2c|v3] {<1-65535>}
```

host <IP>	Configures a host's IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.
[v2c|v3]	Configures the SNMP version used to send the traps • v1 – Uses SNMP version 1. This option is disabled by default. • v2c – Uses SNMP version 2c. This option is disabled by default. • v3 – Uses SNMP version 3. This option is enabled by default.
<1-65535>	Optional. Configures the virtual port of the server resource dedicated to receiving SNMP traps • <1-65535> – Optional. Specify a value from 1 - 65535. The default port is 162.

```
snmp-server manager [all|v1|v2|v3]
```

manager [all|v1|v2|v3]	Enables SNMP manager and specifies the SNMP version • all – Enables SNMP manager version v1, v2 and v3 • 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. • 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. • 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.

```
snmp-server[max-pending-requests {<64-1024>}|request-timeout {<2-720>}]
```

max-pending-requests {<64-1024>}	Sets the maximum number of requests that can be pending at any given time • <64-1024> – Optional. Specify a value from 64 - 1024. The default is 128.
request-timeout {<2-720>}	Sets the interval, in seconds, after which an error message is returned for a pending request • <2-720> – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.

```
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]	Sets the level of suppression of SNMP security configuration information • 0 – If this option is selected, an empty string is returned for the SNMP request for security configuration information. Security configuration information consists of: • Passwords • Keys • Shared secrets The default setting is 0. • 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: • Management policies • IP ACL • Tables containing user names and community strings

```
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 auth md5	Uses SNMP version 3 as the security model • auth – Uses an authentication protocol • md5 – Uses HMAC-MD5 algorithm for authentication
[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures password using one of the following options: • 0 <PASSWORD> – Configures clear text password • 2 <PASSWORD> – Configures encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

```
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des auth md5]
[0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 encrypted	Uses SNMP version 3 as the security model • encrypted – Uses encrypted privacy protocol
auth md5	Uses authentication protocol • auth – Sets authentication parameters • md5 – Uses HMAC-MD5 algorithm for authentication

des auth md5	Uses privacy protocol for user privacy
	• des – Uses CBC-DES for privacy
	  After specifying the privacy protocol, specify the authentication mode.
	• auth – Sets user authentication parameters
	  • md5 – Uses HMAC-MD5 algorithm for authentication

[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	The following are common to both the auth and des parameters: Configures password using one of the following options: • 0 <PASSWORD> – Configures a clear text password • 2 <PASSWORD> – Configures an encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

Examples

```
rfs4000-6DB5D4(config-management-policy-test)#snmp-server community snmp1 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 (management-policy) on page 1555	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <60-300>	Optional. Configures the login grace time. This is the interval, in seconds, after which an unsuccessful login is disconnected. • <60-300> – Specify a value from 60 - 300 seconds. The default is 60 seconds.
port <1-65535>	Optional. Configures the SSH port. This is the port used for SSH connections. • <1-65535> – Specify a value from 1 - 165535. The default port is 22.

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
626b4033263d6d2ae4e79c48cdfcccb60fd4c77a8da9e365060597a6d6570ec2 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

no	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, the T5 controller provides data to WiNG to assist in it's 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 1539.

Supported in the following platforms:

- Wireless Controllers — RFS4000
- Service Platforms — NX9500, NX9600

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]	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.
	• <COMMUNITY-NAME> – Specify the SNMP community name, and configure the access permission for this community string (used by devices to retrieve or modify information).
	  • ro – Allows a remote device to retrieve information only
	  • rw – Allows a remote device to retrieve information and modify settings

<SNMP-STATION-IP>	Specify the SNMP management station IP address for receiving trap information

```
t5 snmp-server contact <LINE>
```

contact <LINE>	Configures the administrator of SNMP trap events for the T5 controller. • <LINE> – Specify the administrator's name (should not exceed 64 characters).

```
t5 snmp-server enable [server|traps]
```

enable [server|traps]	Enables the following: • server – Enables the SNMP server. When enabled, the system accepts SNMP management data. This option is enabled by default. • traps – Enables SNMP traps. When enabled, the system generates SNMP traps. This is enabled by default.

```
t5 snmp-server host <IP>
```

host <IP>	Configures the T5 SNMP host's IP address. The SNMP host receives the SNMP notifications. • <IP> – Specify the SNMP host's IP address.

```
t5 snmp-server location <LINE>
```

location <LINE>	Configures the system location for SNMP traps • <LINE> – Specify the SNMP trap location (should not exceed 64 characters).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <1-65535> – Sets a value from 1 - 165535. The default port is 23.

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 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

no	Disables Telnet

user (management-policy)

Adds a 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Adds a new user account to this management policy • <USERNAME> – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.
password [0 <PASSWORD>| 1 <SHA1-PASSWORD>| <PASSWORD>]	Configures a password for this user • 0 <PASSWORD> – Sets a clear text password • 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password • <PASSWORD> – Sets the password
role	Configures the user role. The options are: • 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. Note: You can restrict a device-provisioning-admin user's access to devices within a specific location or locations, by configuring the allowed-locations parameter (description provided below in this table). • 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. • monitor – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information. • network-admin – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF. • security-admin – Security administrator. Modifies WLAN keys and passphrases. • superuser – Superuser. Has full access, including halt and delete startup-config. • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access. • 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.

access [all|console|ssh| telnet| web]	Configures the services this user can use for remote device access • all – Allows all access types: console, SSH, Telnet, and Web • console – Allows only console access • ssh – Allows only SSH access • telnet – Allows only Telnet access • web – Allows only Web access
allowed-locations <ALLOWED-LOCATIONS>	Optional. This keyword is recursive and optional. It associates an allowed-locations tag with this user. When associated, the user can only access the RF Domains/sites/tree-node paths associated with the specified 'allowed-locations' tag. • <ALLOWED-LOCATIONS> – Specify the allowed-locations tag (should be existing and configured). Note: The "allowed-locations" parameter is only applicable to the WiNGdevice-provisioning-admin role user. Please refer to the Examples: Restricting User Access to Devices in Specific Locations on page 1552 section of this topic for configuration details. Note: Extreme NSight is a separate target, and NSight user accounts and access rights should be configured through the Extreme NSight UI. Note: For information on configuring the allowed-locations tag, see allowed-locations on page 1522.

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role vendor-admin
group <VENDOR-GROUP-NAME>
```

user <USERNAME>	Adds a new user account to this management policy • <USERNAME> – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.
password [0 <PASSWORD>| 1 <SHA1-PASSWORD>| <PASSWORD>]	Configures a password • 0 <PASSWORD> – Sets a clear text password 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password • <PASSWORD> – Sets the password

role vendor-admin	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. 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. 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. **Note:** Use the **service → show → wireless → credential-cache** 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. **Note:** By default the REST server is enabled. For more information, see rest-server.
group <VENDOR-GROUP-NAME>	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 radius-group on page 1558. • <VENDOR-GROUP-NAME> – Provide the vendor group name. In case of multiple allowed groups, provide a list of comma-separated group names.

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 b6b37c51405f4e93c67fe8af82d450c9fd6af69324cd56a55055cefe695b6a14
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
 telnet
 no http server
 https server
```

```
 rest-server
 ssh
 user admin password 1 d9849649218dcaa79109fbd47bbf1a24ecdf1edda220d21f76ce4c15a4e7e696
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)#
```

Examples: Restricting User Access to Devices in Specific Locations

The following set of configurations show how to use the 'allowed-locations' option to permit or deny device-provisioning-admin users access to devices within specific RF Domains/sites.

1 Configure following RF Domains:

a RF Domain 'default' without tree-node.

```
rf-domain default
 country-code us
```

b RF Domain 'California' with tree-node defined as 'Country > Region'.

```
rf-domain California
 no country-code
 tree-node country us region CA
```

c RF Domain 'SanJose' with tree-node defined as 'Country > Region > City'.

```
rf-domain SanJose
 no country-code
 tree-node country us region CA city SJ
```

d RF Domain 'SJCollege' with tree-node defined as 'Country > Region > City > Campus'.

```
rf-domain SJCollege
 no country-code
 tree-node country us region CA city SJ campus SJCollege
```

2 In the Management Policy context,

a Configure following allowed-location tags:

```
management-policy AccessControl
 telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1 superuser role superuser access all
 allowed-location test1 locations US
 allowed-location test2 locations /US/CA/SJ/SJCollege
```

Note

In the above configuration, allowed-location **test1** includes the entire location 'US'. Whereas, allowed-location **test2** only contains the site 'SJCollege'. By assigning 'test1' or 'test2' to a user you can provide access across location 'US' or restrict access to the site 'SJCollege' respectively.

b Configure device-provisioning-admin users and associate the 'allowed-locations' tags (test1 & test2) with each user.

- Create user 'dev-admin' with full access.

```
management-policy AccessControl
 telnet
 no http server
```

```
 https server
 rest-server
 ssh
 user admin password 1 superuser role superuser access all
 user dev-admin password 1 test123 role device-provisioning-admin access all
```

Note
Since allowed-locations parameter has not been specified, this user will have access to all locations 'default', 'California', 'SanJose' and 'SJCollege'.

- Create user 'dev-admin1' with allowed-location 'test1'.

```
management-policy AccessControl
 telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1 superuser role superuser access all
 user dev-admin password 1 test123 role device-provisioning-admin access all
 user dev-admin1 password 1 test112233 role device-provisioning-admin access all
allowed-locations test1
```

Note
Since the allowed-location assigned is 'test1', this user will have access to all RF Domains ('California', 'SanJose' and 'SJCollege') within location 'US'. However, the user will NOT be able to access RF Domain 'default'.

- Configure user 'dev-admin2' with access to allowed-location 'test2'.

```
management-policy AccessControl
 telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1 superuser role superuser access all
 user dev-admin password 1 test123 role device-provisioning-admin access all
 user dev-admin1 password 1 test112233 role device-provisioning-admin access all
allowed-locations test1
 user dev-admin2 password 1 test556677 role device-provisioning-admin access all
allowed-locations test2
```

Note
Since the allowed-location assigned is 'test2', this user's access will be restricted to the location 'SJCollege'.

The following example shows how to restrict a device-provisioning-admin user's access to devices in a specific RF Domain.

1 Configure RF Domain without tree-node:

```
rf-domain Global
 no country-code
```

2 Configure 'allowed-locations' and 'device-provisioning-admin' user as shown in the following output:

```
management-policy AccessControl
 telnet
 http server
 https server
 rest-server
 ssh
```

```
 allowed-location test1 locations US
 allowed-location test2 locations /US/CA/SJ/SJCollege
 allowed-location RFD locations Global
 user admin password 1 superuser role superuser access all
 user dev-admin password 1 test123 role device-provisioning-admin access all
 user dev-admin1 password 1 test112233 role device-provisioning-admin access all
allowed-locations test1
 user dev-admin2 password 1 test556677 role device-provisioning-admin access all
allowed-locations test2
 user dev-admin3 password 1 test8899 role device-provisioning-admin access all allowed-
locations RFD
```

Related Commands

no	Removes a user account configuration

service

Invokes service commands

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • crash-info – Includes an asterix at the end of the prompt if the device has crashfiles in flash:/crashinfo
service show cli	Displays running system information • cli – Displays the current mode's CLI tree

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

17 RADIUS Policy

radius-group
radius-server-policy
radius-user-pool-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:

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 56: RADIUS-Group Config Mode Commands

Command	Description
guest on page 1559	Enables guest access for the newly created group
policy on page 1560	Configures RADIUS group access policy parameters

Table 56: RADIUS-Group Config Mode Commands (continued)

Command	Description
rate-limit on page 1564	Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs
no on page 1565	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1565	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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	Configures access type for a management group. Management groups can be assigned unique access and role permissions. • all – Allows all access. Allows access to the console, ssh, telnet, and/or Web • console – Allows console access only • ssh – Allows SSH access only • telnet – Allows Telnet access only • web – Allows Web access only These parameters are recursive, and you can provide access to more than one component.

```
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]	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: • 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. • 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. • monitor – Monitor. Has read-only access to the network. Can view configuration and statistics except for secret information • 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 • security-admin – Security administrator. Has full read/write access to the network. Modifies WLAN keys and passphrases • superuser – Superuser. Has full access, including halt and delete startup config • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access • 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.

```
policy inactivity-timeout <60-86400>
```

policy inactivity-timeout <60-86400>	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. • <60-86400> – Specify a value from 60 - 86400 seconds. This option is disabled by default.

```
policy session-time <5-144000>
```

policy session-time <5-144000>	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. • <5-144000> – Specify a value from 5 - 144000 minutes. This option is disabled by default. **Note:** For more information, see configuring-device-registration-with-dynamic-vlan-assignment on page 263.

```
policy ssid <SSID>
```

ssid <SSID>	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. • <SSID> – Specify a case-sensitive alphanumeric SSID, not exceeding 32 characters.

```
policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}
```

day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}	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. • fr – Allows access on Friday only • mo – Allows access on Mondays only • sa – Allows access on Saturdays only • su – Allows access on Sundays only • th – Allows access on Thursdays only • tu – Allows access on Tuesdays only • we – Allows access on Wednesdays only • weekdays – Allows access on weekdays only (Monday to Friday

```
policy time start <HH:MM> end <HH:MM>
```

time start<HH:MM> end <HH:MM>	Configures the time when this RADIUS group can access the network • start <HH:MM> – 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. • end <HH:MM> – 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.

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

no on page 1565	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <100-1000000> – Specify the rate from 100 - 1000000 kbps.
from-air <100-1000000>	Sets the rate limit in the uplink direction, from the wireless client to the network • <100-1000000> – Specify the rate from 100 - 1000000 kbps.

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 1565	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *(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 57: RADIUS-Server-Policy Config Mode Commands

Commands	Description
authentication on page 1567	Configures RADIUS authentication settings
bypass on page 1569	Enables bypassing of CRL check
chase-referral on page 1569	Enables LDAP server referral chasing
crl-check on page 1570	Enables a CRL *(certificate revocation list)* check
ldap-agent on page 1571	Configures the LDAP agent settings
ldap-group-verification on page 1573	Enables LDAP group verification
ldap-server on page 1573	Configures the LDAP server settings
local on page 1575	Configures a local RADIUS realm
nas on page 1576	Configures the key sent to a RADIUS client
proxy on page 1577	Configures the RADIUS proxy server's settings
session-resumption on page 1579	Enables session resumption
termination on page 1580	Enables EAP termination on this current RADIUS server policy. When enabled, EAP authentication is terminated at the controller level.
use on page 1581	Defines settings used with the RADIUS server policy
no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication data-source [ldap {fallack}|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 {fallack}|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: **LDAP** and **local**.
ldap fallback	Uses a remote LDAP server as the data source • 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. 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.
local	Uses the local user database to authenticate a user. This is the default setting.
ssid <SSID> precedence <1-5000>	The following keywords are recursive and common to both 'ldap' and 'local' parameters: • ssid – Optional. Associates the data source, selected in the previous step, with a SSID. • <SSID> – 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 (< > | " & \ ? ,). precedence <SSID> – 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. <1-5000> – Specify a precedence from 1 -5000. Note: 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.

```
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 The EAP authentication types supported by the local RADIUS server are: **all**, **peap-gtc**, **peap-mschapv2**, **tls**, **ttls-md5**, **ttls-mschapv2**, **ttls-pap**.
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 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 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • crl-check – Bypasses CRL check of missing CRLs • expired-crl – Bypasses CRL check of expired CRLs **Note:** A CRL is a list of certificates that have been revoked or are no longer valid.

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 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
chase-referral
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-radius-server-policy-test)#chase-referral
```

Related Commands

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • on <DEVICE-NAME> – Optional. Specifies the device name • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. Note: To confirm the join status of a controller, use the **show > ldap-agent > join-status**command.
join-retry-timeout <60-300>	If the join process fails (i.e. the RADIUS server fails to join the LADP server's domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts. • <60-300> – Set the timeout value from 60 - 300 seconds. The default is 60 seconds. Note: A retry timer is initiated as soon as the join process starts, which tracks the time lapse in case of a failure.

```
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 <LDAP-DOMAIN-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-name – Configures the primary or secondary LDAP server's domain name • <LDAP-DOMAIN-NAME> – Specify the domain name.
domain-admin-user <ADMIN-USER-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-admin-user – Configures the primary or secondary LDAP server's admin user name • <ADMIN-USER-NAME> – Specify the admin user's name.

domain-admin-password [0 <WORD>| 2 <WORD>]	This keyword is common to both the 'primary' and 'secondary' parameters.
	• domain-admin-password – Configures the primary or secondary LDAP server's admin user password
	  • 0 <WORD> – Specifies the password in the unencrypted format
	  • 2 <WORD> – Specifies the password in the encrypted format

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

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <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. • <0-600> – Specify a value from 0 - 600 seconds. The default is 300 seconds.

```
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 • <IP> – Specify the LDAP server's IP address.
port <1-65535>	Configures the LDAP server port • <1-65535> – Specify a port between 1 - 65535.
login <LOGIN-NAME>	Configures the login name of a user to access the LDAP server • <LOGIN-NAME> – Specify a login ID (should not exceed 127 characters).
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. • <BIND-DN> – Specify a bind name (should not exceed 127 characters)
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 • <BASE-DN> – Specify a base name (should not exceed 127 characters).

passwd [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Sets a valid password for the LDAP server. • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the LDAP server bind password, specified UNENCRYPTED, with a maximum size of 31 characters
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 <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 <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 <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 groupmembership1 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 groupmembership1 net-timeout 2
 ldap-server dead-period 100nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local realm <RADIUS-REALM>
```

Parameters

```
local realm <RADIUS-REALM>
```

realm <RADIUS-REALM>	Configures a local RADIUS realm • <RADIUS-REALM> – Sets a local RADIUS realm name (a string not exceeding 50 characters)

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 groupmembership1 net-timeout 2
 ldap-server dead-period 100
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <IP/M> – Sets the RADIUS client's IP address in the A.B.C.D/M format
secret [0 <LINE>|2 <LINE>| <LINE>]	Sets the RADIUS client's shared secret. Use one of the following options: • 0 <LINE> – Sets an UNENCRYPTED secret • 2 <LINE> – Sets an ENCRYPTED secret • <LINE> – Defines the secret (client shared secret) up to 64 characters

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

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Configures the realm name • <REALM-NAME> – Specify the realm name. The name should not exceed 50 characters.
server <IP>	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. • <IP> – Sets the proxy server's IP address
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. • <1024-65535> – Sets the proxy server's port from 1024 - 65535 (default port is 1812)
secret [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD> | <PASSWORD>	Sets the proxy server secret string. The options are: • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <ENCRYPTED-PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the proxy server shared secret value

```
proxy retry-count <3-6>
```

retry-count <3-6>	Sets the proxy server's retry count. This is the maximum number of attempts made by a controllers RDIUS server to connect to the proxy server. • <3-6> – Sets a value from 3 - 6 (default is 3 counts)

```
proxy retry-delay <5-10>
```

retry-delay <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. • <5-10> – Sets a value from 5 - 10 seconds (default is 5 seconds)

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 groupmembership1 net-timeout 2
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> {max-entries <10-1024>}	Optional. Sets the lifetime of cached entries • <1-24> – Specify the lifetime period from 1 - 24 hours (default is 1 hour) • max-entries – Optional. Configures the maximum number of entries in the cache <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)
max-entries <10-1024>	Optional. Configures the maximum number of entries in the cache • <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)

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 groupmembership1 net-timeout 2
 session-resumption lifetime 10 max-entries 11
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no on page 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1582	Disables EAP termination on this RADIUS server policy

use

Defines settings used with the RADIUS server policy

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 groupmembership1 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 1582	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [authentication|bypass|chase-referral|clr-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|clr-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 crl-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 58: RADIUS-User-Pool Config Mode Commands

Commands	Description
duration on page 1584	Modifies a guest user's duration of captive-portal access
user on page 1584	Configures the RADIUS user parameters
no on page 1587	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
duration <GUEST-USER-NAME> <0-525600>
```

Parameters

```
duration <GUEST-USER-NAME> <0-525600>
```

duration <GUEST-USER-NAME> <0-525600>	Modifies the duration of captive-portal access (in minutes) for the guest user identified by the <GUEST-USER-NAME> keyword • <GUEST-USER-NAME> – Specify the guest user's name. • <0-525600> – Specify the access duration from 0 - 525600 minutes. A value of "0" indicates unlimited access. The default is 1440 minutes.

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
{group <RAD-GROUP-NAME>} {guest}
user <USERNAME> password [0 <UNECRYPTED-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 <UNECRYPTED-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 <UNECRYPTED-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>	Adds a new RADIUS user to the RADIUS user pool • <USERNAME> – Specify the name of the user. The username should not exceed 64 characters. **Note:** The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.
passwd [0 <UNENCRYPTED-PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures the user password (provide a password unique to this user) • 0 <UNENCRYPTED-PASSWORD> – Sets an unencrypted password • 2 <ENCRYPTED-PASSWORD> – Sets an encrypted password • <PASSWORD> – Sets a password (specified unencrypted) up to 21 characters
group <RAD-GROUP-NAME>	Optional. Configures the RADIUS server group of which this user is a member • <RAD-GROUP-NAME> – Specify the group name in the local database. **Note:** If the user is a guest, assign the user a group with temporary access privileges.
guest	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. A guest user can be assigned only to a guest user group.
expiry-time <HH:MM>	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).
expiry-date <MM:DD:YYYY>	Specify the user account expiry date in the MM:DD:YYYY format (for example. 02:15:2014).

start-time <HH:MM>	Optional. Specify the user account activation time in the HH:MM format.

{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>}	After configuring the above user details, optionally configure the following user information:
	• access-duration <0-525600> – Configures the duration, in minutes, for which this guest user can access the captive portal.
	  • <0-525600> – Specify a value from 0 - 525600 minutes.
	• data-limit <1-102400> – Configures the data limit for which this guest user can access the captive portal. Specify a value from 1 - 102400 bytes.
	  • committed-downlink <100-1000000> – Configures committed downlink 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 downlink rate (specified using this command). Specify a value from 100 - 1000000 Kbps.
	committed-uplink <100-1000000> – 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.
	reduced-downlink <100-1000000> – Configures reduced downlink 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 downlink rate specified here. Specify a value from 100-1000000 Kbps.
	reduced-uplink <100-1000000> – 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.
	• email-id – Optional. User's e-mail ID
	• start-time – Optional. User's account activation time. After specifying the activation time, specify the activation date.
	  • start-date – User's account activation date
	• telephone – Optional. User's telephone number (should include the area code)
	
	To view access details of guest users on a RADIUS server, in the PriviExecutable Configuration mode, use the following command:
	show > radius > 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#`

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

no on page 1587	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no user <USERNAME>
```

Parameters

```
no user <USERNAME>
```

no user <USERNAME>	Deletes a RADIUS user • <USERNAME> – Specify the user name.

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)#
```

18 Radio-QoS Policy

radio-qos-policy-commands

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 then 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 59: Radio-QoS-Policy Config Mode Commands

Command	Description
accelerated-multicast on page 1590	Configures multicast streams for acceleration
admission-control on page 1591	Enables admission control across all radios for one or more access categories
smart-aggregation on page 1595	Configures smart aggregation parameters
service on page 1596	Invokes service commands in the radio QoS configuration mode
wmm on page 1597	Configures 802.11e/wireless multimedia parameters
no on page 1600	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <5-6000>>	Configures a timeout period in seconds for wireless clients • <5-6000> – Specify a value from 5 - 6000 seconds. The default is 60 seconds.
max-client-streams <1-4>	Configures the maximum number of accelerated multicast streams per client • <1-4> – Specify a value from 1 - 4. The default is 2.
max-streams <0-256>	Configures the maximum number of accelerated multicast streams per radio • <0-256> – Specify a value from 0 - 256. The default is 25.
overflow-policy [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: • reject – Rejects new clients. The default overflow policy is reject. • revert – Reverts to regular multicast delivery 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 <1-500>	Configures the number of multicast packets per second threshold value. Once this threshold is crossed, the system triggers streams to accelerate. • <1-500> – Specify a value from 1 - 500. The default is 25 packets per second.

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 1600	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

max-airtime-percent <0-150>	Optional. Specifies the maximum percentage of airtime, including over subscription, for the following access category: • 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. • 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. • 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. • 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. The following keyword is common to all of the above traffic types: • <0-150> – 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%.
max-clients <0-256>	Optional. Specifies the maximum number of wireless clients admitted to the following access categories: • background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio's QoS policy • 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 • video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. • voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. 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. The following keyword is common to all of the above traffic types: • <0-256> – 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.

max-roamed-clients <0-256>	Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category • background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio • best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio • video – Sets the number of video supported wireless clients allowed to roam to a different access point radio • voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio The following keyword is common to all of the above traffic types: • <0-256> – 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.
reserved-for-roam-percent <0-150>	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. • 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. • 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. • 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. • 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. The following keyword is common to all of the above traffic types: • <0-150> – 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%.

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

no on page 1600	Reverts or resets admission control settings to their default

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <0-1000> – Specify a value from 0 - 1000 msec.

```
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 • <1-10> – Specify a value from 1 - 10. The default is 3 hops.

```
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 • <0-64> – Specify a value from 0 - 64. The default is 8 frames.

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 1600	Resets the minimum aggregation limit

service

Invokes service commands in the radio QoS configuration mode

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 admission-control on page 1591.

```
service show cli
```

service show cli	Displays running system information • cli – Displays the Radio QoS mode's CLI tree

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

no on page 1600	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 background	Configures background access category wireless multimedia settings
wmm best-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>	Configures AIFSN *(Arbitrary Inter-Frame Space Number)* as the wait time between data frames derived from the AIFSN and slot time • background – Sets the current AIFSN for low (background) traffic. The default is 7. • best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3. • 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. • 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. The following keyword is common to all of the above traffic types: • <1-15> – Sets a value from 1 - 15
cw-max <0-15>	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. • background – Sets CW Max for low (background) traffic. The default is 10. • best-effort – Sets CW Max for normal (best effort) traffic. The default is 6. • voice – Sets CW Max for voice traffic. The default is 3. • video – Sets CW Max for video traffic. The default is 4 The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). 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).

cw-min <0-15>	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. • background – Sets CW Min for low (background) traffic. The default is 4. • best-effort – Sets CW Min for normal (best effort) traffic. The default is 4. • voice – Sets CW Min for voice traffic. The default is 2. • video – Sets CW Min for video traffic. The default is 3. The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). 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).
txop-limit <0-65535>	Set the interval, in microseconds, during which a particular client has the right to initiate transmissions • background – Sets TXOP for low (background) traffic. The default is 0. • best-effort – Sets TXOP for normal (best effort) traffic. The default is 4. • voice – Sets TXOP for voice traffic. The default is 47. • video – Sets TXOP for video traffic. The default is 94. The following keyword is common to all of the above traffic types: • <0-65535> – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units. 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).

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

no (schedule-policy-config-mode-commands) on page 502	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

19 Role Policy

role-policy-commands

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 60: Role-Policy Config Mode Commands

Command	Description
default-role on page 1603	When a client fails to find a matching role, the default action is assigned to that client
ldap-deadperiod on page 1604	Configures the LDAP *(Lightweight Directory Access Protocol)* dead period interval
ldap-query on page 1605	Enables LDAP service and specifies the LDAP server query mode
ldap-server on page 1606	Configures the LDAP server settings
ldap-timeout on page 1607	Configures the LDAP query timeout
user-role on page 1608	Creates a role and associates it to the newly created role policy
no (role-policy-config-mode-command) on page 1636	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • Use – Associates an IP, IPv6, or MAC access list with the default role
[ip-access-list| ipv6-access-list| mac-access-list] [in|out] <IP/IPv6/MAC-ACCESS-LIST-NAME>	Associates an IP access list, IPv6 access list, or a MAC access list with this default role • in – Applies the rule (IP, IPv6, or MAC) to incoming packets • out – Applies the rule (IP, IPv6, or MAC) to outgoing packets 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 Access-List Policy on page 1353. • <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the access list name. The ACL applied determines the action applied to a client assigned the default role.
precedence <1-100>	The following keyword is common to the all of the above parameters: • precedence – Assigns a precedence value to the ACL identified in the previous step. • <1-100> – Specify a precedence from 1 - 100. ACLs are applied in increasing order of their precedence. Rules with lower precedence are given priority.

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

no (role-policy-config-mode-command) on page 1636	Removes or resets the default role configuration

ldap-deadperiod

Configures LDAP dead period interval

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ldap-deadperiod <60-300>
```

Parameters

```
ldap-deadperiod <60-300>
```

ldap-deadperiod <60-300>	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 ldap-query on page 1605 command. • <60-300> – Specify the interval from 60 - 600 seconds. The default is 120 seconds.

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

no (role-policy-config-mode-command) on page 1636	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ldap-query [self|through-controller]
```

Parameters

```
ldap-query [self|through-controller]
```

self	Configures LDAP query mode as **self**. The AP directly queries the LDAP server for user information. Select 'self' to use local LDAP server resources configured using the ldap-server on page 1606 command.
through-controller	Configures LDAP query mode as **through-controller**. 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

no (role-policy-config-mode-command) on page 1636	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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:
	• server-type – Optional. Specifies the LDAP server type
	  • active-directory – Enables support for active directory attribute search. This is the default setting.
	  • openldap – Enables support for openLDAP attribute search

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

no (role-policy-config-mode-command) on page 1636	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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) 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

no (role-policy-config-mode-command) on page 1636	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <ROLE-NAME> Specify a name for this user role.
precedence <1-10000>	Sets the precedence for this role **Note:** 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.

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

no (role-policy-config-mode-command) on page 1636	Removes an existing user role from the role policy

user-role commands

The following table summarizes the user role configuration commands:

Table 61: User-Role-Mode Commands

Commands	Description
ap-location on page 1610	Configures an AP deployment location based filter
assign on page 1611	Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role
authentication-type on page 1613	Configures an authentication type based filter
captive-portal on page 1614	Configures a captive portal based filter
city on page 1615	Configures a city name based filter
client-identity on page 1616	Associates a client-identity (device fingerprinting) based filter
company on page 1617	Configures a company name based filter
country on page 1618	Configures a country name based filter
department on page 1619	Configures a department name based filter
emailid on page 1620	Configures a e-mail ID based filter
employee-type on page 1621	Configures a employee type ID based filter
employeeid on page 1622	Configures a employee ID based filter
encryption-type on page 1623	Configures an encryption type filter
group on page 1624	Configures a RADIUS group based filter
memberOf on page 1625	Assigns an *Active Directory* (AD) group to this user-defined role
mu-mac on page 1626	Configures MAC address and mask based filter
radius-user on page 1627	Configures a wireless client filter based on the RADIUS user name
ssid on page 1628	Configures a SSID based filter
state on page 1629	Configures a user role state to match
title on page 1630	Configures a 'title' string to match
use on page 1631	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 on page 1634	Defines a filter based on an attribute defined in the Active Directory or the OpenLDAP server
no (user-role-config-mode-command) on page 1635	Removes or resets the filters configured on this user-defined role

ap-location

Configures an AP's deployment location based filter for this user-defined role

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **contains**, **exact**, or **not-contains**.
contains <WORD>	Applies role if the associating AP's location contains the location string specified in the role. • <WORD> – Specify the location string to match.
exact <WORD>	Applies role if the associating AP's location exactly matches the string specified in the role. • <WORD> – Specify the exact location string to match.
not-contains <WORD>	Applies role if the associating AP's location does not contain the location string specified in the role. • <WORD> – Specify the location string. The role is applied if the location does not match the specified string.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)}
```

eq [eap| kerberos| mac-auth|none]	The role is applied only when the authentication type matches (equals) one or more than one of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used **Note:** These parameters are recursive, and you can configure more than one unique authentication type for this user-defined role.
neq [eap| kerberos| mac-auth|none]	The role is applied only when the authentication type does not match (not equals) any of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used **Note:** These parameters are recursive, and you can configure more than one unique 'not equal to' authentication type for this user-defined role.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. 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 This option requires the wireless client to share authentication credentials after logging into the managed network.
pre-login	Specifies authentication is pending 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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contain**.
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. • <WORD> – 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.

exact <WORD>	The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
not-contains <WORD>	The role is applied only when the city name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – 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.

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

no	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.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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) • <CLIENT-IDENTITY-NAME> – Specify the client identity signature name. **Note:** Multiple client identities can be configured with a role policy.

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

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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. • <WORD> – 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.
exact <WORD>	The role is applied only when the company name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
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. • <WORD> – 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.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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. • <WORD> – 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.
exact <WORD>	The role is applied only when the country name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
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. • <WORD> – 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.

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

no	Removes the country name configured with this user-defined role

department

Configures a wireless client filter based on the department name

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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. • <WORD> – 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.
exact <WORD>	The role is applied only when the department name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
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. • <WORD> – 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.

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

no	Removes the department 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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 <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – 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.
exact <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
not-contains <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. • <WORD> – 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.

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

no	Removes the e-mail ID 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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 <WORD>	The role is applied only when the employee type, returned by the RADIUS server, contains the string specified in the role. • <WORD> – 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.
exact <WORD>	The role is applied only when the employee type, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
not-contains <WORD>	The role is applied only when the employee type, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – 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.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
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. • <WORD> – 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.
exact <WORD>	The role is applied only when the employee ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
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. • <WORD> – 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.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)}
```

eq [ccmp|keyguard|none||wep128|wep64]	The role is applied only if the encryption type equals to one of the following options: • ccmp: Encryption mode is CCMP • keyguard: Encryption mode is keyguard. Keyguard encryption shields the master encryption keys from being discovered • none: No encryption mode specified • tkip – Encryption mode is TKIP • wep128: Encryption mode is WEP128 • wep64: Encryption mode is WEP64 Note: These parameters are recursive, and you can configure more than one encryption type for this user-defined role.
neq [ccmp|keyguard|none|wep128|wep64]	The role is applied only if encryption type is not equal to any of the following options: • ccmp: Encryption mode is not equal to CCMP • keyguard: Encryption mode is not equal to keyguard • none: Encryption mode is not equal to none • tkip – Encryption mode is not equal to TKIP • wep128: Encryption mode is not equal to WEP128 • wep64: Encryption mode is not equal to WEP64 Note: These parameters are recursive, and you can configure more than one 'not equal to' encryption type for this user-defined role.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
any	This user-defined role can fit into any group (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the RADIUS group name contains the string specified in the role. • <WORD> – 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.
exact <WORD>	The role is applied only when the RADIUS group name exactly matches the string specified in the role. • <WORD> – 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.
not-contains <WORD>	The role is applied only when the RADIUS group name does not contain the string specified in the role. • <WORD> – 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.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
memberOf <AD-GROUP-NAME>
```

Parameters

```
memberOf <AD-GROUP-NAME>
```

memberOf <AD-GROUP-NAME>	Applies this user-defined role to a client only if the client belongs to the specified AD group • <AD-GROUP-NAME> – Specify the AD group name.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mu-mac [<MAC>|any]
mu-mac any
mu-mac <MAC> {mask <MAC>}
```

Parameters

```
mu-mac any
```

any	Applies role to any wireless client (no MAC address to match). This is the default setting.

```
mu-mac <MAC> {mask <MAC>}
```

<MAC>	Applies role to the wireless client having specified MAC address • <MAC> – Sets the MAC address in the AA-BB-CC-DD-EE-FF format
mask <MAC>	Optional. After specifying the client's MAC address, specify the mask in the • AA-BB-CC-DD-EE-FF format. The role is applied to the wireless client exactly matching the specified MAC address and MAC mask.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – 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. Note: You can use the realm or any sub-string of the user name.
ends-with <WORD>	Enables role assignment on the basis of the wireless client's "department" and/or "group" • <WORD> – 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. Note: The role is applied only when the 'radius-user' name, returned by the RADIUS server, ends with the string specified here.

exact <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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. Note: Provide the complete user name along with the realm.
not-contains <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – 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.
starts-with <WORD>	Enables role assignment on the basis of the wireless client's "department" and/or "group" code • <WORD> – 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. Note: The role is applied only when the 'radius-user' name, returned by the RADIUS server, starts with the string specified here.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
ssid [any|exact|contains|not-contains]
ssid any
ssid [exact|contains|not-contains] <WORD>
```

Parameters

```
ssid any
```

ssid any	Specifies a wireless client filter based on how the SSID is specified in a WLAN. • any – The role is applied to any SSID location. This is the default setting.

```
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: **contains**, **exact**, or **not-contains**.
exact <WORD>	The role is applied only when the SSID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
not-contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the SSID string not to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
any	This user role can fit any wireless client irrespective of the state (no strings to match).
contains <WORD>	The user role is applied only when the RADIUS state contains the string specified in the role. • <WORD> – 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.
exact <WORD>	The role is applied only when the RADIUS state exactly matches the string specified in the role. • <WORD> – 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.
not-contains <WORD>	The role is applied only when the RADIUS state does not contain the string specified in the role. • <WORD> – 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.

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

no	Removes the 'state' filter string associated with a user role

title

Configures a 'title' string to match

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **any**, **contains**, **exact**, or **not-contains**.
any	This user role can fit any wireless client irrespective of the title (no strings to match).
contains <WORD>	The user role is applied only when the title string, returned by the RADIUS server, contains the string specified in the role. • <WORD> – 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.
exact <WORD>	The role is applied only when the title string, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – 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.
not-contains <WORD>	The role is applied only when the title string, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – 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.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-list|
mac-access-list|purview-application-policy|url-filter]

use [application-policy|bonjour-gw-discovery-policy|purview-application-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|purview-application-policy]
```

application-policy <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. • <POLICY-NAME> – Specify the Application policy name (should be existing and configured). **Note:** For more information on Application policy, see application-policy on page 195.
bonjour-gw-discovery-policy <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. • <POLICY-NAME> – Specify the Bonjour GW Discovery policy name (should be existing and configured). **Note:** Ror more information on Bonjour GW Discovery policy, see bonjour-gw-discovery-policy on page 219.
purview-application-policy <PURVIEW-APP-POLICY-NAME>	Uses an existing Purview application policy with this user role. When associated, the application policy enforces application assurance for all users using this role. • <PURVIEW-APP-POLICY-NAME> – Specify the Application policy name (should be existing and configured). **Note:** For more information on Purvoew application policy, see purview-application-policy on page 436.

```
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 • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<IPv4/IPv6-ACCESS-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. • <1-100> – Sets a precedence from 1 - 100

```
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 • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<MAC-ACCESS-LIST-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. • <1-100> – Sets a precedence from 1 - 100

```
use url-filter <URL-FILTER-NAME>
```

use url-filter <URL-FILTER-NAME>	Uses an existing URL filter that acts as a Web content filter firewall rule. • <POLICY-NAME> – Specify the URL filter name (should be existing and configured).

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <ATTR-NAME> – Specify the attribute string. 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 <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, contains the string specified in the role. • <WORD> – 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.
exact <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. • <WORD> – 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.
not-contains <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. • <WORD> – 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.

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

no	Removes the user-defined filter configured with this user role

no (user-role-config-mode-command)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (role-policy-config-mode-command)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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=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)#
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)#
```

20 SMART-RF Policy

smart-rf-policy commands

This chapter summarizes *Self-Monitoring at Run Time RF* (SMART 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 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.

Note

Starting with the WiNG 7.2.0 release, SMART RF is supported on the AP510i/e and AP560i/h model access points running in the dual-5GHz mode. For setting access point RF mode, see rf-mode on page 1129.

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 62: Smart-RF-Policy Config Mode Commands

Command	Description
area on page 1641	Configures the channel list and power for a specified area
assignable-power on page 1642	Specifies the power range during power assignment
avoidance-time on page 1642	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.
channel-list on page 1644	Assigns the channel list for the selected frequency
channel-width on page 1645	Selects the channel width for Smart RF configuration
coverage-hole-recovery on page 1646	Enables recovery from errors
enable on page 1648	Enables the Smart RF policy
group-by on page 1648	Configures grouping parameters
interference-recovery on page 1649	Enables recovery from excessive noise and interference related issues
neighbor-recovery on page 1651	Enables recovery from faulty neighbor radios related issues
select-shutdown on page 1653	Enables selection and shutting down of 2.4 GHz radios, causing interference, in case the CCI *(co-channel interference)* value exceeds a specified threshold
sensitivity on page 1655	Configures Smart RF sensitivity parameters
smart-ocs-monitoring on page 1656	Applies smart OCS *(off-channel scanning)* instead of dedicated detectors
no (smart-rf-policy-config-mode-command) on page 1660	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Specifies the area name • <AREA-NAME/STRING-ALIAS> – 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. **Note:** For more information on aliases, see alias on page 172.
channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>	Selects the channels for the specified area in the 2.4 GHz or 5.0 GHz band • 2.4GHz – Selects the channels for the specified area in the 2.4 GHz band • 5GHz – Selects the channels for the specified area in the 5.0 GHz band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <CHANNEL-LIST> – Enter a comma-separated list of channels for the selected band.

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

no (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • max <1-20> – Sets the upper limit from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit from 1 dBm - 20 dBm (default is 4 dBm)
5GHz [max|min] <1-20>	Assigns a power range on the 5.0 GHz band • max <1-20> – Sets the upper limit from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit from 1 dBm - 20 dBm (default is 4 dBm)

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

no (smart-rf-policy-config-mode-command) on page 1660	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 1100.

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 1108.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
avoidance-time [adaptivity|dfs] <30-3600>
```

Parameters

```
avoidance-time [adaptivity|dfs] <30-3600>
```

avoidance-time [adaptivity|dfs] <30-3600>	Configures the time for which a channel is avoided after dfs or adaptivity is triggered • adaptivity – Sets the time, in minutes, for which a radio avoids an adaptivity-regulated channel detected with interference • dfs – Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected on radar • <30-3600> – Specify a value from 30 - 3600 minutes. The default for both parameters is 90 minutes.

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

no (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <WORD> – Specify a comma separated list of channels
5GHz <WORD>	Assigns a channel list for the 5.0 GHz band • <WORD> – Specify a comma separated list of channels

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

no (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • 20MHz – Assigns the 20 MHz channel width. This is the default setting. • 40MHz – Assigns the 40 MHz channel width • auto – Auto-selects the channel. Assigns the best possible channel in the 20 MHz or 40 MHz channel width.

```
channel-width 5GHz [20MHz|40MHz|auto]
```

channel-width 5GHz [20MHz|40MHz|auto]	Assigns the channel width for the 5.0 GHz band • 20MHz – Assigns the 20 MHz channel width. • 40MHz – Assigns the 40 MHz channel width. This is the default setting. • 80MHz – Assigns the 80 MHz channel width • auto – Auto-selects the channel. Assigns the best possible channel in the 20 MHz or 40 MHz or 80 MHz channel width.

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

no (smart-rf-policy-config-mode-command) on page 1660	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 1655.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-255> – Sets a value from 1 - 255. The default is 1.
5GHz <1-255>	Specifies the minimum number of clients on the 5.0 GHz band • <1-255> – Sets a value from 1 - 255. The default is 1.

```
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 <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 2.4GHz <1-120> – Specifies the coverage hole recovery interval on the 2.4 GHz band • <1-120> – Specify a value from 1 - 120 seconds. Note: coverage-interval – The default is 10 seconds. Note: interval – The default is 30 seconds.
5GHz <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 5GHz <1-120> – Specifies a coverage hole recovery interval on the 5.0 GHz band • <1-120> – Specify a value from 1 - 120 seconds. Note: coverage-interval – The default is 10 seconds. Note: interval – The default is 30 seconds.

```
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>	Specifies SNR threshold on the 2.4 GHz band • <1-75> – Sets a value from 1 dB - 75 dB. The default is 20 dB.
5GHz <1-75>	Specifies SNR threshold on the 5.0 GHz band • <1-75> – Sets a value from 1 - 75. The default is 20 dB.

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 (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 **Note:** 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

no (smart-rf-policy-config-mode-command) on page 1660	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 1655.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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| 5GHz]	Selects the band • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<5-35>	Specifies the threshold value for the difference between the current and prospective channel interference levels • <5-35> – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.

```
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 • <0-86400> – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 1,800 seconds.
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. • <1-255> – Sets the number of clients from 1 - 255. The default is 50.
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. • <3-10> – Specify a noise factor value from 3 - 10.

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 • <1.0-3.0> – Specify the noise factor from 1.0 - 3.0. The default is 1.5.

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

no (smart-rf-policy-config-mode-command) on page 1660	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 1655.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <1-10> – Sets the number of retries from 1 - 10. The default is 3.
threshold <1-30>	Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling • <1-30> – Sets the minimum number of reports from 1 - 30. The default is 5.

```
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 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 • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<-85--55>	Specify the threshold value • <-85--55> – 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.

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 (smart-rf-policy-config-mode-command) on page 1660	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 enabled one-by-one 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, AP7632, AP7662, AP-8432, AP-8533
- Wireless Controllers — RFS 4000
- Service Platforms — NX 5500, NX 75XX, NX 95XX, NX 96XX, VX

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 • <-85--55> – Specify a value from -85 - -55 dBm. The default value is -80 dBm. **Note:** If not specified, the system uses the default value as the upper limit.
cci-low-threshold <-100--55>	Optional. Configures the minimum CCI threshold • <-100--55> – Specify a value from -100 - -55 dBm. The default value is -100 dBm. **Note:** If not specified, the system uses the default value as the lower limit.
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. • <0-3600> – Specify the frequency from 0 - 3600 minutes. The default is 60 minutes.
frequency-limiter <1-1000>	Configures the minimum multiple of Interference Recovery frequency that the select-shutdown frequency can be set to • <1-100> – Specify a value from 1 - 1000. The default value is 15.

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 (smart-rf-policy-config-mode-command) on page 1660	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}	Configures a time and day schedule when awareness settings are overridden • <1-3> – Sets the awareness override schedule index. A maximum of three overrides can be configured. • <START-TIME> – Sets the override start time in HH:MM format • <END-TIME> – Sets the override end time in HH:MM format DAY – Optional. Set the day when the override is active. Use one of the following formats: all – Override is active on all days sun – Override is active only on Sundays mon – Override is active only on Mondays tue – Override is active only on Tuesdays wed – Override is active only on Wednesdays thu – Override is active only on Thursdays fri – Override is active only on Fridays sat – Override is active only on Saturdays

```
smart-ocs-monitoring {awareness-override threshold <10-10000>}
```

awareness-override threshold <10-10000>	Optional. Use this parameter to configure client awareness settings overrides • threshold – Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden. • <10-10000> – Specify a threshold value from 10 -10000. The default is 10.

```
smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}
```

client-aware	Optional. Enables client aware scanning on this Smart RF policy Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals this threshold number, 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). This feature is disabled by default.
2.4GHz <1-255>	Enables client aware scanning on the 2.4 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 50 clients.
5GHz <1-255>	Enables client aware scanning on the 5.0 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 50 clients.

```
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 • <0-50> – Sets the number of trails from 0 - 50. The default is 5.
5GHz <0-50>	Enables extended scan on the 5.0 GHz band • <0-50> – Sets the number of trails from 0 - 50. The default is 5.

```
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 • <1-120> – Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.
5GHz <1-120>	Selects the 5.0 GHz band • <1-120> – Sets a scan frequency from 1 sec - 120 sec. The default is 6 seconds.

```
smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}
```

off-channel-duration	Optional. Specifies the duration to scan off channel 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 <20-150>	Selects the 2.4 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 milliseconds. The default is 50 milliseconds.
5GHz <20-150>	Selects the 5.0 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 milliseconds. The default is 50 milliseconds.

```
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. This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio.
2.4GHz [disable|dynamic|strict]	Sets power save aware scanning mode on the 2.4 GHz band • disable – Disables voice awareness scanning • dynamic – Dynamically avoids scanning based on traffic for power save (PSP) clients. This is the default setting. • strict – Strictly avoids scanning when PSP clients are present
5GHz [disable|dynamic|strict]	Sets power save aware scanning mode on the 5.0 GHz band • disable – Disables voice awareness .scanning • dynamic – Dynamically avoids scanning based on traffic for PSP clients. This is the default setting. • strict – Strictly avoids scanning when voice PSP are present

```
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 • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 10
5GHz <1-15>	Selects the 5.0 GHz band • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 5.

```
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 • <1-100> – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.
5GHz <1-100>	Selects the 5.0 GHz band • <1-100> – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.

```
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: **disable**, **dynamic**, and **strict**. 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 • disable – Disables voice awareness scanning • dynamic – Dynamically avoids scanning based on traffic for voice clients. This is the default setting. • strict – Strictly avoids scanning when voice clients are present
5GHz [dynamic|strict]	Specifies the scanning mode on the 5.0 GHz band • dynamic – Dynamically avoids scanning based on traffic for voice clients. This is the default setting. • strict – Strictly avoids scanning when voice clients are present.

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

no (smart-rf-policy-config-mode-command) on page 1660	Disables off-channel monitoring

no (smart-rf-policy-config-mode-command)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

21 WIPS Policy

wips-policy-commands

This chapter summarizes the *Wireless Intrusion Protection Systems* (WIPS) 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 *mobile units* (MUs) 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, deauth, 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, see use (rf-domain-config-mode) on page 488.

Note

With this most recent release, AP7522 and AP7532 model access points can provide enhanced sensor support. AP7522 and AP7532 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

AP7522 and AP7532 models also support shared part-time scanning using WIPS in WiNG (using off-channel-scans) and not ADSP. WIPS on WiNG is enhanced to add rogue detection/classification (wired side detection based of MAC Address Offset) and OTA *(over-the-air)* termination for AP7522 and AP7532 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 63: WIPS-Policy Config Mode Commands

Command	Description
ap-detection on page 1665	Defines the WIPS AP detection configuration
enable on page 1667	Enables the WIPS policy
event on page 1667	Configures events
history-throttle-duration on page 1671	Configures the duration event duplicates are omitted from the event history
interference-event on page 1671	Specifies events contributing to the Smart RF WiFi interference calculations
signature on page 1672	Configures a WIPS policy signature and enters its configuration mode
use on page 1682	Defines a WIPS policy settings
no (wips-policy-config-mode-command) on page 1683	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <30-86400> – Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).
recurring-event-interval <0-10000>	Configures recurring event interval help of unauthorized APs • <0-10000> – Configures the recurring interval between 0 - 10000 seconds. The default is 300 seconds.
interferer-threshold <-100--10>	Configures RSSI threshold value to determine if an unsanctioned ap is an interferer or not • <-100--10> – Configures the rssi threshold between -100 - -10 dBm. The default is -75 dBm.
wait-time <10-600>	Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed • <10-600> – Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).

```
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. • allow-channel-switch – Optional. Allows channel switch of unauthorized APs based on the channel mode. This option is disabled by default. • mode [auto|manual] – Optional. Select the mode as **auto** or **manual** to configure. The default setting is manual.

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

no (wips-policy-config-mode-command) on page 1683	Resets unauthorized or unsanctioned AP detection settings to default

enable

Enables this WIPS policy

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
enable
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-wips-policy-test)#enable
```

Related Commands

no (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]

event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
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|asleap|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]
```

ap-anomaly	Enables AP anomaly event tracking 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
asleap	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 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>	The following keywords are common to all of the above client anomaly events: • filter-ageout <0-86400> – Optional. Configures the filter expiration time in seconds • <0-86400> – Sets the filter ageout time from 0 - 86400 seconds. The default is 0 seconds. Note: 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. 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.

```
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 <0-86400>	The following keywords are common to all excessive events: • filter-ageout <0-86400> – 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. • <0-86400> – Sets a filter ageout time from 0 - 86400 seconds. The default is o seconds. Note: 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.
threshold-client <0-65535>	The following keywords are common to all excessive events: • threshold-client <0-65535> – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a wireless client threshold value from 0 - 65535 seconds
threshold-radio <0-65535>	The following keywords are common to all excessive events: • threshold-radio <0-65535> – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a radio threshold value from 0 - 65535 seconds

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 (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
history-throttle-duration <30-86400>
```

Parameters

```
history-throttle-duration <30-86400>
```

history-throttle-duration <30-86400>	Configures the duration event duplicates are omitted from the event history • <30-86400> – Sets a value from 30 - 86400 seconds. The default is 120 seconds.

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

no (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
signature <SIGNATURE-NAME>
```

Parameters

```
signature <SIGNATURE-NAME>
```

signature <SIGNATURE-NAME>	Configures a WIPS policy signature • <SIGNATURE-NAME> – Enter a name for the WIPS policy signature. The name should not exceed 64 characters.

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

no (wips-policy-config-mode-command) on page 1683	Deletes a WIPS policy signature

signature mode commands

The following table summarizes WIPS policy signature configuration mode commands:

Table 64: WIPS-Policy-Signature Config Mode Commands

Commands	Description
bssid on page 1674	Configures the BSSID MAC address
dst-mac on page 1674	Configures the destination MAC address
filter-ageout on page 1675	Configures the filter ageout interval
frame-type on page 1676	Configures the frame type used for matching
interference-event on page 1677	Configures this WIPS policy signature as the Smart RF interference source

Table 64: WIPS-Policy-Signature Config Mode Commands (continued)

Commands	Description
mode on page 1677	Enables the signature mode
payload on page 1678	Configures payload settings
src-mac on page 1678	Configures the source MAC address
ssid-match on page 1679	Configures a match based on SSID
threshold-client on page 1680	Configures the wireless client threshold limit
threshold-radio on page 1680	Configures the radio threshold limit
no (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|reassoc]
```

Parameters

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|
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 1679.

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

no (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wips-policy-config-mode-command) on page 1683	Disables this WIPS policy signature as Smart RF interference source

mode

Enables this WIPS policy signature

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (wips-policy-config-mode-command) on page 1683	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
payload <1-3> pattern <WORD> offset <0-255>
```

Parameters

```
payload <1-3> pattern <WORD> offset <0-255>
```

payload <1-3>	Configures payload settings • <1-3> – Set the payload index from 1 - 3.
pattern <WORD>	Specifies the pattern to match: hex or string • <WORD> – Set the pattern name.
offset <0-255>	Specifies the payload offset to start the pattern match • <0-255> – Set the offset value from 0 - 255.

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

no (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
src-mac <MAC>
```

Parameters

```
src-mac <MAC>
```

src-mac <MAC>	Configures the source MAC address to match • <MAC> – Specify the source MAC address.

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

no (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <SSID> – Specify the SSID string. Note: Specify the correct SSID to ensure proper filtering.
ssid-len <0-32>	Specifies the length of the SSID • <0-32> – Specify the SSID length from 0 - 32 characters.

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 (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
threshold-client <1-65535>
```

Parameters

```
threshold-client <1-65535>
```

threshold-client <1-65535>	Configures the client threshold limit • <1-65535> – Set the threshold limit for a 60 second window from 1 - 65535.

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

no (wips-signature-config-mode-command) on page 1681	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
threshold-radio <1-65535>
```

Parameters

```
threshold-radio <1-65535>
```

threshold-radio <1-65535>	Configures the radio's threshold limit • <1-65535> – Specify the threshold limit for a 60 second window from 1 - 65535.

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

no (wips-signature-config-mode-command) on page 1681	Removes the radio's threshold limit configured with a WIPS policy signature

no (wips-signature-config-mode-command)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode|payload|
src-mac|ssid-match|threshold-client|threshold-radio]
no [bssid|dts-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)
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use device-categorization <DEVICE-CATEGORIZATION>
```

Parameters

```
use device-categorization <DEVICE-CATEGORIZATION>
```

device-categorization <DEVICE-CATEGORIZATION>	Associates a device categorization list • <DEVICE-CATEGORIZATION> – Specify the device categorization object name to associate with this WIPS policy.

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

no (wips-policy-config-mode-command) on page 1683	Disables the use of a device categorization policy with a WIPS policy

no (wips-policy-config-mode-command)

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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|
asleap|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)#
```

22 WLAN-QoS Policy

WLAN-QOS-Policy commands

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 65: WLAN-QoS-Policy-Config Commands

Command	Description
accelerated-multicast on page 1686	Configures accelerated multicast stream addresses and forwards QoS classifications
classification on page 1687	Classifies WLAN traffic based on priority
multicast-mask on page 1689	Configures the egress prioritization multicast mask
qos on page 1690	Defines the QoS configuration
rate-limit on page 1690	Configures the WLAN traffic rate limit using a WLAN QoS policy
svp-prioritization on page 1693	Enables Spectralink voice protocol support on a WLAN
voice-prioritization on page 1693	Prioritizes voice client over other clients
wmm on page 1694	Configures 802.11e/wireless multimedia parameters
no (wlan-qos-policy-config-mode-command) on page 1697	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
multicast-mask [primary|secondary] <MAC/MASK>
```

Parameters

```
multicast-mask [primary|secondary] <MAC/MASK>
```

primary <MAC/MASK>	Configures the primary egress prioritization multicast mask • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX-XX format Note: Setting masks is optional and only needed if there are traffic types requiring special handling.
secondary <MAC/MASK>	Configures the primary egress prioritization multicast mask • <MAC/MASK> – Sets the MAC address and the mask in the AA-BB-CC-DD-EE-FF / XX-XX-XX-XX-XX-XX-XX format

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)#
```

qos

Enables QoS on this WLAN

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
qos trust [dscp|wmm]
```

Parameters

```
qos trust [dscp|wmm]
```

trust [dscp|wmm]	Trusts the QoS values of ingressing packets • dscp – Trusts the IP DSCP values of ingressing packets • wmm – Trusts the 802.11 WMM QoS values of ingressing packets

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <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. Note: 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 <0-100>	The following is common to the 'from-air' and 'to-air' parameters: 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 <0-100>	The following is common to the 'from-air' and 'to-air' parameters: 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: 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: 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 *Unscheduled Automatic Power Save Delivery* (U-APSD), is specifically designed for WMM voice devices.
qbss-load-element	Enables support for the *QOS Basic Service Set* (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 *Arbitrary Inter-Frame Space Number* (AIFSN) from 2 - 15. AIFSN is the wait time between data frames. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 2 The default for traffic best effort (normal) categories is 3 The default for traffic background (low) categories is 7 • <2-15> – Sets a value from 2 - 15
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. The default for traffic voice categories is 3 The default for traffic video categories is 4 The default for traffic best effort (normal) categories 10 The default for traffic background (low) categories is 10 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.
cw-min <0-15>	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. The default for traffic voice categories is 2 The default for traffic video categories is 3 The default for traffic best effort (normal) categories is 4 The default for traffic background (low) categories is 4 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.
txop-limit <0-65535>	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. The default for traffic voice categories is 47 The default for traffic video categories is 94 The default for traffic best effort (normal) categories is 0 The default for traffic background (low) categories is 0 • <0-65535> – Set a value from 0 - 65535 to configure the transmit-opportunity in 32 microsecond units.

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)#
```

no (wlan-qos-policy-config-mode-command)

Removes this WLAN QoS Policy settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]	Disables accelerated multicast streams and forwarding QoS classification • <IP> – Removes specified IP address. Specify the IP address • autodetect – Disables multicast streams automatic detection
no classification [non-unicast| non-wmm]	Disables WLAN classification scheme • non-unicast – Optional. Removes multicast and broadcast packet classification • non-wmm – Optional. Removes non-WMM client traffic classification
no multicast-mask [primary|secondary]	Disables the egress prioritization primary or secondary multicast mask • primary – Removes the first egress multicast mask • secondary – Removes the second egress multicast mask
no qos trust [disquiet]	Disables the QoS service • trust – Ignores the trust QOS values of ingressing packets • dscp – Ignores the IP DSCP values of ingressing packets • wmm – Ignores the 802.11 WMM QoS values of ingressing packets

no svp-prioritization	Disables *Spectralink Voice Protocol* (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 [client|wlan]	Disables traffic rate limit parameters • Disables client traffic rate limits • Disables WLAN traffic rate limits
[from-air|to-air]	The following are common to the client and WLAN parameters: • from-air – Removes client/WLAN traffic rate limits in the up link direction. This is traffic from the wireless client to the network • to-air – Removes client/WLAN traffic rate limits in the down link direction. This is traffic from the network to the wireless client
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 • background – Disables the low priority traffic (background) threshold value • best-effort – Disables the normal priority traffic (best effort) threshold value • video – Disables the video traffic threshold value • voice – Disables the voice traffic threshold value

```
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 [backgorund|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:

```
nx9500-6C8809nx9500-6C8809(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)#
```

23 L2TPv3 Policy

l2tpv3-policy-commands
l2tpv3-tunnel-commands
l2tpv3-manual-session-commands

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 de-multiplex 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 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.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the psuedowire 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

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 66: L2TPV3-Policy-Config Commands

Command	Description
cookie-size on page 1702	Configures the cookie field size for each L2TPV3 data packet
failover-delay on page 1703	Configures the L2TPV3 tunnel failover delay in seconds
force-12-path-recovery on page 1704	Enables the forced detection of servers and gateways behind the L2TPV3 tunnel
hello-interval on page 1705	Configures the interval, in seconds, between L2TPV3 "Hello" keep-alive messages exchanged in the L2TPV3 control connection
reconnect-attempts on page 1705	Configures the maximum number of retransmissions for signalling messages
reconnect-interval on page 1706	Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection
retry-attempts on page 1707	Configures the maximum number of retransmissions of signalling messages
retry-interval on page 1707	Configures the interval, in seconds, before initiating a retransmission of any L2TPV3 signaling message
rx-window-size on page 1708	Configures the number of signaling messages received without sending an acknowledgment
tx-window-size on page 1709	Configures the number of signaling messages transmitted without receiving an acknowledgment
no (l2tpv3-policy-config-mode-command) on page 1709	Removes this L2TPv3 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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • 0 – No cookie field present in each L2TPV3 data message (this is the default setting) • 4 – 4 byte cookie field present in each L2TPV3 data message • 8 – 8 byte cookie field present in each L2TPV3 data message

Examples

```
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#cookie-size 8
<exsw1>(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 cookie-size 8
nx9500-6C8809(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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) • <5-60> – Specify a fail-over delay from 5 - 60 seconds. The default is 5 seconds.

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

no	Resets the failover interval to its default (5 seconds)

force-12-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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
force-12-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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
hello-interval <1-3600>
```

Parameters

```
hello-interval <1-3600>
```

hello-interval <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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <0-8> – Specify a value from 0 - 8 (default is 0: configures infinite reconnect attempts).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-3600> – Specify a value from 1 - 3600 seconds (default is 120 seconds).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
retry-interval <1-250>
```

Parameters

```
retry-interval <1-250>
```

retry-interval <1-250>	Configures the interval, in seconds, between two successive retransmission attempts • <1-250> – Specify a value from 1 - 250 seconds (default is 5 seconds).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-15> – Specify a value from 1 - 15 (default is 10 packets).

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (l2tpv3-policy-config-mode-command)

Removes this L2TPv3 policy settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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-<device-name>)#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
  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 67: L2TPV3-Tunnel-Config Commands

Command	Description
establishment-criteria on page 1711	Configures L2TPV3 tunnel establishment criteria
fast-failover on page 1713	Configures fast-failover support on the L2TPv3 tunnel
hostname on page 1714	Configures tunnel specific local hostname
local-ip-address on page 1714	Configures the tunnel's IP address
mtu on page 1715	Configures the tunnel's MTU *(Maximum Transmission Unit)* size
peer on page 1715	Configures the tunnel's peers
preempt on page 1719	Enables preemption of secondary tunnel when primary tunnel comes back. And, configures the interval after which the the secondary tunnel is preempted.
router-id on page 1720	Configures the tunnel's local router ID
session on page 1721	Creates/modifies specified L2TPV3 session
use on page 1722	Configures a tunnel to use a specified L2TPV3 tunnel policy
no (l2tpv3-tunnel-config-mode-command) on page 1723	Removes this L2TPv3 tunnel settings or reverts them to default value

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, 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>]
```

always	Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting. 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 **Note:** 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 **Note:** 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 • <1-255> – Specify the VRRP group number from 1 - 255. **Note:** 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-Tunnel1)#establishment-
criteria
cluster-master
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)#
```

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. **Note:** The hello-interval and retry-attempts parameters are defined in the L2TPv3 Policy context. For more information on configuring an L2TPv3 policy, see l2tpv3-policy-commands on page 1701. For more information on associating an L2TPv3 policy to an L2TPv3 tunnel, see use on page 1722.

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

no (l2tpv3-tunnel-config-mode-command) on page 1723	Removes fast-failover support on the L2TPv3 tunnel

hostname

Configures the tunnel's local hostname

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
hostname <WORD>
```

Parameters

```
hostname <WORD>
```

hostname <WORD>	Configures the tunnel's local hostname • <WORD> – Specify the tunnel's local hostname.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local-ip-address <IP>
```

Parameters

```
local-ip-address <IP>
```

local-ip-address <IP>	Configures the L2TPv3 tunnel's source IP address • <IP> – 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.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mtu <128-1460>
```

Parameters

```
mtu <128-1460>
```

mtu <128-1460>	Configures the MTU size for this tunnel • <128-1460> – Specify a value from 128 - 1460 bytes (default is 1460 bytes).

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Configures the tunnel's peer ID • <1-2> – 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. **Note:** 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 fast-failover on page 1713.
hostname [<HOSTNAME>|any]	Optional. Configures the peers' hostname. The hostname options are: • <HOSTNAME> – Specifies the hostname as FQDN *(Fully Qualified Domain Name)* or partial DN or any other name • 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.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer hostname, optionally specify the IPSec settings: • ipsec-secure – Optional. Enables auto IPSec on the L2TPv3 tunnel • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: <IP> – Configures IPSec gateway's IP address <WORD> – Configures IPSec gateway's hostname

router-id [<IP>|<WORD>|any]	After specifying the peer hostname, optionally specify router ID settings:
	• router-id – Optional. Configures the peer's router ID in one of the following formats:
	  • <IP> – Peer router ID in the IP address (A.B.C.D) format
	  • <WORD> – Peer router ID range (for example, 100-120)
	  • any – Peer router ID is not specified. This allows incoming connection from any router ID.

udp {ipsec-secure gw|port <1-65535> {ipsec-secure}}	After specifying the peer hostname, optionally specify UDP settings:
	The UDP option configures the encapsulation mode for this tunnel.
	• UDP – Optional. Configures UDP encapsulation (default encapsulation is IP)
	  • ipsec-secure gw – Optional. Enables auto IPSec
	  • port <1-65535> {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.

```
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 • <IP> – Specify the peer's IP address.
hostname [<FQDN>|any]	After specifying the peer IP address, optionally specify the peer's hostname: Optional. Configures the peers' hostname. The hostname options are: • <FQDN> – Specifies the hostname as FQDN or partial DN • 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.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer IP address, optionally specify the IPSec settings: • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: <IP> – Configures IPSec gateway's IP address <WORD> – Configures IPSec gateway's hostname

router-id [<A.B.C.D>| <WORD>| any]	After specifying the peer IP address, optionally specify the router ID using one of the following options:
	• router-id – Optional. Configures the peer's router-id in one of the following formats:
	  • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format
	  • <WORD> – Peer router ID range (for example, 100-120)
	  • any – Peer router ID is not specified. This allows incoming connection from any router ID.

udp {ipsec-secure gw|port <1-65535> {ipsec-secure}}	After specifying the peer IP address, optionally specify the peer's UDP port settings:
	The UDP option configures the encapsulation mode for this tunnel.
	• UDP – Optional. Configures UDP encapsulation (default encapsulation is IP)
	  • ipsec-secure gw – Optional. Enables auto IPSec
	  • port <1-65535> – 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.

```
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 [<IP>|<WORD>]}	Optional. Enables auto IPSec for this peer
	• gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:
	  • <IP> – Configures IPSec gateway's IP address
	  • <WORD> – Configures IPSec gateway's hostname

```
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 [<A.B.C.D>| <WORD>| any]	Optional. Configures the peer's router-id in one of the following formats: • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) • any – Peer router ID is not specified. This allows incoming connection from any router ID.

ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer's router ID, optionally specify the IPSec settings. • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: <IP> – Configures IPSec gateway's IP address <WORD> – Configures IPSec gateway's hostname
udp {ipsec-secure gw| port <1-65535> {ipsec-secure}}	After specifying the peer's router ID, optionally specify the IPSec settings. The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> – 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.

```
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| port <1-65535> {ipsec-secure}}	Optional. Configures UDP encapsulation for this tunnel's pee (default encapsulation is IP) • ipsec-secure – Optional. Configures IPSec gateway on this peer UDP port • port <1-65535> – 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.

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, in case the primary tunnel goes down. This command also configures the delay time in preemption of the secondary tunnel.

Use this command to configure the time to wait before preempting the secondary tunnel.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • delay <60-600> – Specify a value from 60 - 600 seconds. The default is 60 seconds.

Examples

```
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnel1)#preemption delay 100
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnel1)#show context
 l2tpv3 tunnel tunnel1
  preempt enable
  preemption delay 100
nx9500-6C8809(config-profile test-l2tpv3-tunnel-tunnel1)#
```

Related Commands

no (l2tpv3-tunnel-config-mode-command) on page 1723	Disables preemption of secondary tunnel when primary tunnel comes back

router-id

Configures the tunnel's local router ID

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
router-id [<1-4294967295>|<IP>]
```

Parameters

```
router-id [<1-4294967295>|<IP>]
```

router-id [<1-4294967295>| <IP>]	Configures the tunnel's local router ID in one of the following formats: • <1-4294967295> – Router ID in the number format (from1- 4294967295) • <IP> – Router ID in IP address format (A.B.C.D)

Examples

```
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#router-id 2000
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
```

```
  peer 2 hostname tunnel1peer1 udp port 100
  router-id 2000
  establishment-criteria cluster-master
nx9500-6C8809(config-profile default-rfs4000-l2tpv3-tunnel-Tunnel1))#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <L2TPV3-SESSION-NAME> – 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.
pseudowire-id <1-4294967295>	Configures the pseudowire ID for this session from 1- 4204067295 A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (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 • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35).
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

```
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 • <L2TPV3-SESSION-NAME> – 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.
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. • 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 • 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)
rate <50-1000000>	Specify the data rate, in kilobits per second, for the incoming and/or outgoing traffic • <50-1000000> – Specify a value from 50 - 1000000 kbps. The default is 5000 Kbps.
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. • <2-1024> – 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.

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 tunnel1peer1 udp port 100
  use l2tpv3-policy L2TPV3Policy1
  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 the L2TPV3 policy configured with a tunnel and reverts to the default tunnel policy

no (l2tpv3-tunnel-config-mode-command)

Removes this L2TPv3 tunnel settings or reverts them to default value

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [establishment-criteria|fast-failover|hostname|local-ip-address|mtu|peer <1-2>|preempt|
router-id|session|use]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Negates or reverts a L2TPv3 tunnel settings to default, based on the parameters passed

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 68: L2TPV3-Manual-Session-Config Commands

Command	Description
local-cookie on page 1725	Configures the manual session's local cookie field size
local-ip-address on page 1726	Configures the manual session's local source IP address
local-session-id on page 1727	Configures the manual session's local session ID
mtu on page 1727	Configures the MTU size for the manual session tunnel
peer on page 1728	Configures the manual session's peers
remote-cookie on page 1729	Configures the remote cookie for the manual session
remote-session-id on page 1730	Configures the manual session's remote session ID
traffic-source on page 1730	Configures the traffic source tunneled by the manual session
no (l2tpv3-manual-session-config-mode-command) on page 1731	Negates or reverts L2TPV3 manual session commands to default

local-cookie

Configures the local cookie field size for the manual session

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

Parameters

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

local-cookie size [4|8]	Configures the local cookie field size for this manual session. The options are: • 4 – 4 byte local cookie field • 8 – 8 byte local cookie field
<1-4294967295>	Configures the local cookie value first word. Applies to both the 4 byte and 8 byte local cookies
<1-4294967295>	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
local-ip-address <IP>
```

Parameters

```
local-ip-address <IP>
```

local-ip-address <IP>	Configures the manual session's source IP • <IP> – Specify the IP address in the A.B.C.D format.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-63> – 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.

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. 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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mtu <128-1460>
```

Parameters

```
mtu <128-1460>
```

mtu <128-1460>	Configures the MTU size for this manual session • <128-1460> – Specify a value from 128 - 1460 bytes (default is 1460 bytes).

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. The peers are identified by their IP addresses.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
peer ip-address <IP> {udp {port <1-65535>}}
```

Parameters

```
peer ip-address <IP> {udp {port <1-65535>}}
```

peer ip-address <IP>	Configures the session peer's IP address in the A.B.C.D format
udp {port <1-65335>}	Optional. Configures the UDP encapsulation mode for this session (default encapsulation is IP) • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service. • <1-65335> – Specify a value from 1 - 65535.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • 4 – 4 byte remote cookie field • 8 – 8 byte remote cookie field
<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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
remote-session-id <1-4294967295>
```

Parameters

```
remote-session-id <1-4294967295>
```

remote-session-id <1-4294967295>	Configures this manual session's remote ID • <1-4294967295> – Specify a value from 1 - 4294967295.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <VLAN-ID-RANGE>	Configures VLAN as the traffic source for this tunnel • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35)
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

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

no	Removes the traffic source configured for a manual session

no (l2tpv3-manual-session-config-mode-command)

Removes this L2TPV3 manual session settings or reverts them to default value

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|
remote-session-id|traffic-source]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	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)#
```

24 Router Mode

router-mode-commands

This chapter summarizes *Open Shortest Path First* (OSPF) router mode commands in the CLI command structure. All router-mode commands are available on both device and profile modes.

OSPF is an *interior gateway protocol* (IGMP) 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 69: OSPF-Router Config Mode Commands

Command	Description
area on page 1734	Specifies OSPF enabled interfaces
auto-cost on page 1740	Specifies the reference bandwidth in terms of Mbits per second
default-information on page 1741	Controls the distribution of default information
ip on page 1742	Configures IP *IInternet Protocol)* default gateway priority
network on page 1743	Defines OSPF network settings
ospf on page 1744	Enables OSPF
passive on page 1745	Specifies the configured OSPF interface as passive interface
redistribute on page 1745	Specifies the route types redistributed by OSPF
route-limit on page 1746	Specifies the limit for the number of routes managed by OSPF
router-id on page 1748	Specifies the router ID for OSPF
no (router-mode-config-command) on page 1748	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 616.

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 defined as: stub area, totally-stub, non-stub, nssa, totally nssa. Each of these area types have been discussed further in the area-type topic 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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 • <0-4294967295> – Specify the value from 0 - 4294967295.
<IP>	Defines an OSPF area in the form of an IP address • <IP> – Specify the IP address.

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 70: OSPF-Area-Mode Commands

Command	Description
area-type on page 1736	Configures a particular OSPF area as STUB or NSSA
authentication on page 1737	Specifies the authentication scheme used for the OSPF area
range on page 1738	Specifies the routes matching address/mask for summarization
no (area-config-mode-command) on page 1739	Removes this area settings
no (router-mode-config-command) on page 1748	Removes this area configuration from the router mode policy

area-type

Configures a particular OSPF area as STUB, Totally STUB, NSSA or Totally NSSA. Areas can defined as:

- stub area - Is an area that does not receive route advertisements external to the AS *(autonomous system)*, 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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 STUB *Stubby Area*
default-cost <0-16777215>	Specifies the default summary cost advertised, if the OSPF area is a STUB or NSSA • <0-16777215> – Specify the default summary cost value from 0 - 16777215.
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

no (area-config-mode-command) on page 1739	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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

no (area-config-mode-command) on page 1739	Removes the authentication scheme assoictaed 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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

Syntax

```
range <IP/M>
```

Parameters

```
range <IP/M>
```

<IP/M>	Specifies the routes matching address/mask for summarization. Note: 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

no (area-config-mode-command) on page 1739	Removes the configured network IP range

no (area-config-mode-command)

Removes this OSPF area settings

Supported in the following platforms:

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

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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

Syntax

```
auto-cost reference-bandwidth <1-4294967>
```

Parameters

```
auto-cost reference-bandwidth <1-4294967>
```

reference-bandwidth <1-4294967>	Defines the reference bandwidth in Mbps • <1-4294967> – Specify the reference bandwidth value from 1 - 4294967.

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 (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 <0-16777214>	This is a recursive parameter and can be optionally configured along with the metric-type option. • metric <0-16777214> – Optional. Specifies OSPF metric value for redistributed routes (this value is used to generate the default route) • <0-16777214> – Specify a value from 0 - 16777214.

metric-type [1|2]	This is a recursive parameter and can be optionally configured along with the metric option.
	• metric-type [1|2] – Optional. Sets OSPF exterior metric type for redistributed routes (this information is advertised with the OSPF routing domain)
	  • 1 – Sets OSPF external type 1 metrics
	  • 2 – Sets OSPF external type 2 metrics

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

no (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 • <1-8000> – Specify an integer from 1 - 8000. The default is 7000. **Note:** Lower the value, higher is the priority.

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 (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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: • <0-4294967295> – Specifies a 32 bit OSPF area ID from 0 - 4294967295 • <IP> – Defines an OSPF area ID in the form of an IPv4 address

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

no (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

Syntax

```
ospf enable
```

Parameters

```
ospf enable
```

ospf enable	Enables OSPF routing on devices using this profile. This option is disabled by default.

Examples

```
nx9500-6C8809(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

no (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 • <1-4094> – Specify the VLAN interface ID from 1 - 4094.

Examples

```
nx9500-6C8809(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

no (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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: • metric <0-16777214> – Optional. Specifies the OSPF metric value for redistributed routes. • <0-16777214> – Specify a value from 0 - 16777214.

metric-type[1|2]	The following keywords are common to the 'connected', 'kernel', and 'static' parameters:
	• metric-type [1|2] – Optional. Sets the OSPF exterior metric type for redistributed routes
	  • 1 – Sets the OSPF external type 1 metrics
	  • 2 – Sets the OSPF external type 2 metrics

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 (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

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 <DYNAMIC-ROUTE-LIMIT>	Specifies the maximum number of non self-generated LSAs this process can receive • <DYNAMIC-ROUTE-LIMIT> – Specify the dynamic route limit.
reset-time <1-86400>	Specifies the time, in seconds, after which the retry-count is reset to zero • <1-86400> – Specify a value from 1 - 86400 seconds. The default is 360 seconds.
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. • <1-32> – Specify a value from 1 - 32. The default is 5.
retry-timeout <1-3600>	Specifies the retry time in seconds. During this time, OSPF remains in ignore state and all adjacencies are suppressed. • <1-3600> – Specify a value from 1 - 3600 seconds. The default is 60 seconds.

Examples

```
nx9500-6C8809(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

no (router-mode-config-command) on page 1748	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 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP 7622, AP-8163, AP-8432, AP-8533
- Wireless Controllers — RFS 4000

Syntax

```
router-id <IP>
```

Parameters

```
router-id <IP>
```

<IP>	Identifies the OSPF router by its IP address • <IP> – Specify the router ID in the IP <A.B.C.D> format

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 (router-mode-config-command) on page 1748	Removes the configured OSPF router ID

no (router-mode-config-command)

Removes this OSPF router settings or reverts them to default values

Supported in the following platforms:

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

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)#
```

25 Routing Policy

routing-policy-commands

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 71: Routing-Policy-Config Commands

Command	Description
apply-to-local-packets on page 1751	Enables PBR for locally generated packets
logging on page 1752	Enables logging for a specified route map
route-map on page 1752	Creates a route map entry
use on page 1761	Defines default settings to use
no (routing-policy-config-mode-command) on page 1762	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no (routing-policy-config-mode-command) on page 1762	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (routing-policy-config-mode-command) on page 1762	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-100> – Specify a precedence value from 1 - 100. Note: Lower the sequence number, higher is the precedence.

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 72: Route-Map-Config Commands

Command	Description
default-next-hop on page 1755	Sets the default next hop for packets satisfying match criteria
fallback on page 1756	Configures a fallback to the next destination
mark on page 1756	Marks action clause for packets satisfying match criteria
match on page 1757	Sets match clauses for the route map
next-hop on page 1759	Sets the next hop for packets satisfying match criteria

Table 72: Route-Map-Config Commands (continued)

Command	Description
no (route-map-config-mode-command) on page 1760	Removes the route-map settings or reverts them to default values
no (routing-policy-config-mode-command) on page 1762	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]
```

default-next--hop	Sets the next hop router to which packets are sent in case the next hop is not the adjacent router
<IP>	Specifies next hop router's IP address
<ROUTER-IF-NAME>	Specifies the outgoing interface name (router interface name)
pppoe1	Specifies the PPPoE interface
serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>	Specifies the serial interface's slot, port, and channel group IDs
vlan <1-4094>	Specifies a VLAN interface ID • <1-4094> – Specify a value from 1 - 4094.
wwan1	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 (route-map-config-mode-command) on page 1760	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (route-map-config-mode-command) on page 1760	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
mark ip dscp <0-63>
```

Parameters

```
mark ip dscp <0-63>
```

ip dscp <0-63>	Marks the DSCP field in the IP header • <0-63> – Specify a DSCP value from 0 - 63.

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 (route-map-config-mode-command) on page 1760	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 1756. And for more information on fallback action, see fallback on page 1756.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> <CHANNEL-GROUP-ID>	Specifies the serial interface's slot, port, and channel group IDs.
vlan <1-4094>	Specifies the VLAN interface ID • <1-4094> – Specify a VLAN ID from 1 - 4094.
wwan1	Specifies the WAN interface name

```
match ip dscp <0-63>
```

ip dscp <0-63>	Sets the DSCP match clause • <0-63> – Specify a value from 0 - 63. The defined DSCP value is used as a matching clause for this route map.

```
match ip-access-list <IP-ACCESS-LIST-NAME>
```

ip-access-list <IP-ACCESS-LIST-NAME>	Sets the match clause using a pre-configured IP access list • <IP-ACCESS-LIST-NAME> – Specify a pre-configured IP access list name.

```
match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>
```

wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>	Sets the wireless client role match clause • <ROLE-POLICY-NAME> – Specify a pre-configured role policy. • <ROLE-NAME> – Specify a pre-configured role within it.

```
match wlan <WLAN-NAME>
```

wlan <WLAN-NAME>	Sets the incoming WLAN match clause • <WLAN-NAME> – Specify a WLAN name.

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

no (route-map-config-mode-command) on page 1760	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 Note: 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 • <1-4094> – Specify a VLAN ID from 1 - 4094. The VLAN interface should be a DHCP client.
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 (route-map-config-mode-command) on page 1760	Disables the next hop router settings

no (route-map-config-mode-command)

Removes this route-map settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 (routing-policy-config-mode-command) on page 1762	Disables CRM link status monitoring

no (routing-policy-config-mode-command)

Removes this Routing policy settings or reverts them to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

26 AAA-TACACS Policy

aaa-tacacs-policy-commands

This chapter summarizes the *accounting, authentication, and authorization* (AAA) *Terminal Access Control Access-Control System* (TACACS) 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 73: AAA TACACS Policy Configuration Commands

Command	Description
accounting on page 1764	Configures TACACS accounting parameters
authentication on page 1767	Configures TACACS authentication parameters

Table 73: AAA TACACS Policy Configuration Commands (continued)

Command	Description
authorization on page 1769	Configures TACACS authorization parameters
no (aaa-tacacs-policy-config-mode-command) on page 1772	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 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>	Sets the scaling factor for retry timeouts • <50-200> – Specify a value from 50 - 200. The default is 100. A value of 100 indicates the time gap between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry.

```
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 • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server port (the port used to connect to the accounting server) • <1-65535> – Specify the TCP accounting port number from 1 - 65535. The default port is 49.

```
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. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
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. • <1-3> – Specify a value from 1 - 3. The default is 3.

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 (aaa-tacacs-policy-config-mode-command) on page 1772	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. Note: 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 • <1-2> – Specify the TACACS server index from 1 - 2.
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 • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authentication port from 1 - 65535. The default port is 49.

```
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 • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures timeout scaling between two consecutive TACACS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

```
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 • <1-2> – Specify the TACACS server index from 1- 2.
timeout <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. • <3-60> – Specify a value from 3- 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10. The default is 3.

```
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 **Note:** 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 (aaa-tacacs-policy-config-mode-command) on page 1772	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-2> – Specify the TACACS server index from 1 - 2.
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 • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authorization port from 1 - 65535. The default port is 49.

```
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 • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between consecutive TACACS authorization retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

```
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 • <1-2> – Specify the TACACS server's index from 1- 2.
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. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
attempts <1-3>	Optional. Indicates the number of retry attempts to make before giving up • <1-3> – Specify a value from 1 - 3. The default is 3.

```
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 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 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 (aaa-tacacs-policy-config-mode-command) on page 1772	Resets values or disables commands

no (aaa-tacacs-policy-config-mode-command)

Removes this AAA TACACS policy settings or revrets to default values

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
no [accounting|authentication|authorization]
```

Parameters

```
no <PARAMETERS>
```

no <PARAMETERS>	Removes this AAA TACACS policy settings or revrets 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:

```
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)#
nx9500-6C8809(config-aaa-tacacs-policy-test)#no authentication directed-request
nx9500-6C8809(config-aaa-tacacs-policy-test)#no accounting auth-fail
nx9500-6C8809(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:

```
nx9500-6C8809(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting commands
nx9500-6C8809(config-aaa-tacacs-policy-test)#
```

27 Meshpoint Policy

meshpoint-config-instance
meshpoint-qos-policy-config-instance
meshpoint-device-config-instance

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.

Note
The WiNG 7.1.X release does not support Meshpoint configuration on AP5XX model access points. This feature will be supported in future releases.

This chapter is organized as follows:

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
allowed-vlans (meshpoint-config) on page 1775	Configures VLANs allowed on the meshpoint
beacon-format (meshpoint-config) on page 1776	Configures the beacon format for the meshpoint AP
control-vlan (meshpoint-config) on page 1777	Configures the VLAN where meshpoint control traffic traverses
data-rates (meshpoint-config) on page 1778	Configures the data rates supported per frequency band
description (meshpoint-config) on page 1782	Configures a human friendly description for this meshpoint
force (meshpoint-config) on page 1783	Forces formation of sub-optimal paths through the meshpoint's root node
meshid (meshpoint-config) on page 1783	Configures a unique ID for this meshpoint
neighbor (meshpoint-config) on page 1784	Configures the neighbor inactivity time out for this meshpoint
root (meshpoint-config) on page 1785	Configures a meshpoint as the root meshpoint

Command	Description
security-mode (meshpoint-config) on page 1787	Configures the security mode on the meshpoint.
service (meshpoint-config) on page 1788	Allows only 802.11n capable neighbors to create a mesh connection
shutdown (meshpoint-config) on page 1789	Shuts down the meshpoint
use (meshpoint-config) on page 1789	Associates a QoS policy with this meshpoint
wpa2 (meshpoint-config) on page 1790	Configures WPA2 encryption settings
no (meshpoint-config) on page 1794	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 on page 616.

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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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. 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). • <VLAN-ID> – Specify the VLAN ID or the range of IDs to add.
remove <VLAN-ID>	Removes a single VLAN or a range of VLANs from the list of allowed VLANs. • <VLAN-ID> – Specify the VLAN ID or the range of IDs to remove.

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

no (meshpoint-config) on page 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 1794	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 meshpont roots. Once configured, the control VLAN carries the mesh point's control traffic.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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>]	Configures the control VLAN • <1-4094> – Specify the control VLAN from 1 - 4094. The default is VLAN 1. • <VLAN-ALIAS-NAME> – Uses a vlan-alias to specify the control vlan. If using a vlan-alias, ensure that it is existing and configured. 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. **Note:** Control VLAN need not necessarily be added in the allowed VLAN list.

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 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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	Configures the preset data rates for the 2.4 GHz frequency Define both minimum **Basic** and optimal **Supported** 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. 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. 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.
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)	Configures custom rates • 1 – Configures the available rate at 1 Mbps • 2 – Configures the available rate at 2 Mbps • 5.5 – Configures the available rate at 5.5 Mbps • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 11 – Configures the available rate at 11 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps • basic-mcs0-7 – Configures the MCS index range of 0 - 7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates

```
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	Configures the preset data rates for the 5.0 GHz frequency Define both minimum **Basic** and optimal **Supported** 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. 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.
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)	Configures custom rates • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps • basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates.

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

no (meshpoint-config) on page 1794	Resets data rates for each frequency band for this meshpoint

description (meshpoint-config)

Configures a brief description for this meshpoint

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 **Note:** 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

no (meshpoint-config) on page 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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. • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 120 seconds.

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

no (meshpoint-config) on page 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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)#ap81xx 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

no (meshpoint-config) on page 1794	Removes the configuration of this meshpoint device as a root meshpoint

security-mode (meshpoint-config)

Configures the security mode for this meshpoint

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
security-mode [eap|none|psk]
```

Parameters

```
security-mode [eap|none|psk]
```

security-mode	Configures the security mode for this meshpoint
eap	Uses 802.1X/EAP as the security mode. When using this option, use the wpa2 command to specify the EAP authentication type and related parameters.
none	No security is configured for this meshpoint
psk	Uses PSK *(Pre Shared Key* as the security mode. When using this option, use the wpa2 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

no (meshpoint-config) on page 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
service [allow-ht-only|show cli]
```

Parameters

```
service [allow-ht-only|show cli]
```

service allow-ht-only	Allows only those neighbors who are capable of high throughput data rates (802.11n data rates) to associate with the meshpoint
service show cli	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

no (meshpoint-config) on page 1794	Removes the restriction that only 802.11n capable neighbor devices can associate with this meshpoint
service on page 623 (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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
shutdown
```

Parameters

```
None
```

Examples

```
nx9500-6C8809(config-meshpoint-test)#shutdown
```

Related Commands

no (meshpoint-config) on page 1794	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 <MESHPOINT-QOS-POLICY-NAME>	Configures this meshpoint to use a predefined meshpoint QoS policy • <MESHPOINT-QOS-POLICY-NAME> – Specify the meshpoint QoS policy name (should be existing and configured).
aaa-policy <AAA-POLICY-NAME>	Configures this meshpoint to use a predefined aaa-policy • <AAA-POLICY-NAME> – Specify the aaa-policy name (should be existing and configured).

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

no (meshpoint-config) on page 1794	Removes the meshpoint QoS policy associated with this meshpoint
meshpoint-qos-policy-config-instance on page 1795	Creates and configures a meshpoint QoS policy
AAA Policy on page 1303	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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>
```

wpa2 key-rotation	Enables periodic rotation of encryption keys used for broadcast and unicast traffic
broadcast	Configures key rotation interval for broadcast and multicast traffic. This option is disabled by default. 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.
unicast	Configures key rotation interval for unicast traffic. This option is disabled by default.
<30-86400>	Configures key rotation interval from 30 - 86400 seconds for unicast or broadcast transmission

```
wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]
```

wpa2 psk	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.
secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures the PSK used to authenticate this meshpoint with other meshpoints in the network • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – 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.

```
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]	Specifies the EAP authentication type. The options are: • peap-mschapv2 – Configures EAP authentication type as PEAP *(Protected Extensible Authentication Protocol)* with default auth type MSCHAPv2. This is the default setting. If using auth-type as 'peap-mschapv2', use the 'peap-mschapv2' keyword to configure user credentials and trustpoint details. • tls – Configures EAP authentication type as TLS *(Transport Layer Security)* If using auth-type as 'tls', use the 'tls' keyword to configure trustpoint details. Note: 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.
identity <WORD>	Configures identity to be used during phase1 authentication • <WORD> – Enter a string up to 256 characters in length (this should not be actual identity of user but some anonymous/bogus username).

```
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>]	Specify the user credentials used for authentication • user <USER-NAME> – Specify the user name • password [0 <WORD>|2 <WORD>|<WORD>] – Specify the password associated with the specified user.
trustpoint <TRUSTPOINT-NAME>	Optional. Associates a trustpoint used for installing CA certificate and verifying server certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured).

```
wpa2 eap tls trustpoint <TRUSTPOINT-NAME>
```

wpa2 eap tls	Configures TLS client related parameters
trustpoint <TRUSTPOINT-NAME>	Configures trustpoint details trustpoint • <TRUSTPOINT-NAME> – Assigns a trustpoint to be used for installing TLS client certificate, client private key, and CA certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured)

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

no (meshpoint-config) on page 1794	Resets PSK configuration and key rotation duration

no (meshpoint-config)

Negates meshpoint commands or resets their values to default

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 1773.

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 74: Meshpoint-QoS-Policy Config Mode Commands

Command	Description
accelerated-multicast (meshpoint-qos-policy) on page 1797	Configures accelerated multicast parameters
rate-limit (meshpoint-qos-policy) on page 1798	Configures the rate limits for this QoS policy
no (meshpoint-qos-policy) on page 1801	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 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: • background • best effort • trust • video • voice

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

no (meshpoint-qos-policy) on page 1801	Resets accelerated multicast configurations for this meshpoint QoS policy

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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 <2-1024>	Optional. Configures the maximum burst size in kilobytes. • <2-1024> – Set a value from 2 - 1024 kbytes. 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. 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.
rate <50-1000000>	Optional. Defines a receive or transmit rate limit in kilobytes per second • <50-1000000> – Set a value from 50 - 1000000 kbps. 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. 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.

```
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 <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • background <0-100> – Configures the threshold for low priority (background) traffic • <0-100> – Specify a value from 0 - 100. 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%. 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%.

best-effort <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • best-effort <0-100> – Configures the threshold for best-effort traffic • <0-100> – Specify a value from 0 - 100. 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%. 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%.
video <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • best-effort <0-100> – Configures the threshold for video traffic • <0-100> – Specify a value from 0 - 100. 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%. 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%.
voice <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • voice <0-100> – Configures the threshold for voice traffic • <0-100> – Specify a value from 0 - 100. 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%. 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.

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

no (meshpoint-qos-policy) on page 1801	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

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 `mespoint-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 75: Meshpoint-Device Config Commands

Command	Description
acs (meshpoint-device-config) on page 1803	Enables ACS *(Automatic Channel Selection)* on this meshpoint device (access point)
exclude (meshpoint-device-config) on page 1808	Excludes neighboring mesh devices
hysteresis (meshpoint-device-config) on page 1809	Configures path selection SNR hysteresis values on this meshpoint-device (Access Point)
monitor (meshpoint-device-config) on page 1810	Enables monitoring of critical resource and primary port links on a meshpoint device
path-method (meshpoint-device-config) on page 1811	Configures the method used to select the path to the root node in a mesh network
preferred (meshpoint-device-config) on page 1812	Configures the preferred path parameters for a meshpoint device
root (meshpoint-device-config) on page 1814	Configures a meshpoint device as the root meshpoint
root-select (meshpoint-device-config) on page 1813	Configures this meshpoint device as the cost root
no (meshpoint-device-config) on page 1815	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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>	Configures the minimum time, in seconds, before a periodic scan, to assess channel conditions for a meshpoint root, is triggered. • 2.4 GHz – Configures the channel hold interval for the 2.4 GHz radio band • 5.0GHz – Configures the channel hold interval for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <0-86400> – Specify a value from 0 - 86400 seconds. The default is 1800 seconds. **Note:** A value of '0' disables periodic channel assessment.

```
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>	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. • 2.4 GHz – Configures the channel switch delta for the 2.4GHz radio band • 5.0GHz – Configures the channel switch delta for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <5-35> – Specify a value from 5 - 35 dBm. The default is 10 dBm.

```
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]	Configures the channel width that meshpoint auto channel selection assigns to the radio • 2.4 GHz – Configures the operating channel width for the 2.4 GHz radio band • 5.0 GHz – Configures the operating channel width for the 5.0 GHz radio band The following keywords are common to the '2.4 GHz' and '5.0 GHz' bands: • 20 MHz – Assigns the 20 MHz channel width to the radio • 40 MHz – Assigns the 40 MHz channel width to the radio • auto – Selects and assigns the best possible channel from the 20/40 MHz width. This is the default setting.

```
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>	Configures the duration, in milliseconds, of OCSs *(off -channel scans)* • 2.4 GHz – Configures the ocs-duration for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-duration for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <20-250> – Specify a value from 20 - 250 milliseconds. The default value is 50 milliseconds.

```
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>	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. • 2.4 GHz – Configures the ocs-frequency for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-frequency for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-60> – Specify a value form 1 - 60 seconds. The default is 6 seconds.

```
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>	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. • 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band • 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <100-20000> – Specify a value from 100 - 20000. The default is 1000.

```
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>	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. • 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <800-65535> – Specify a value from 800 -65535. The default is 1500.

```
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>	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. • 2.4 GHz – Configures the maximum tolerance period for the 2.4 GHz radio band • 5.0 GHz – Configures the maximum tolerance period for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <800-65535> – Specify a value from 10 - 600 seconds.

```
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>	Configures the preferred radio interface on dual band APs • 2.4 GHz – Configures the preferred radio interface for the 2.4 GHz radio band • 5.0 GHz – Configures the preferred radio interface for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <0-2> – Specify a value form 0 - 2. A value of 0 (zero) indicates no preferred radio.

```
acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>	Configures the priority meshpoint. Configuring a priority meshpoint overrides automatic meshpoint configuration. • 2.4 GHz – Configures the priority meshpoint for the 2.4 GHz radio band • 5.0 GHz – Configures the priority meshpoint for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <MESHPOINT-NAME> – Specify the meshpoint name for the selected radio band.

```
acs sample-count [2.4GHz|5GHz] <1-10>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
sample-count [2.4GHz|5GHz] <1-10>	Configures the minimum number of scan cycle samples to consider for auto channel selection • 2.4 GHz – Configures the sample count for the 2.4 GHz radio band • 5.0 GHz – Configures the sample count for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-10> – Specify a value from 1 -10. The default is 5 samples.

```
acs snr-delta [2.4GHz|5GHz] <1-100>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
snr-delta [2.4GHz|5GHz] <1-100>	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. • 2.4 GHz – Configures the snr-delta for the 2.4 GHz radio band • 5.0 GHz – Configures the snr-delta for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-100> – Specify a value from 1 - 100 dB. The default is 5 dB.

```
acs snr-threshold [2.4GHz|5GHz] <-100-0>
```

acs	Configures ACS settings and overrides on the selected meshpoint-device
snr-threshold [2.4GHz|5GHz] <-100-0>	Configures the signal strength threshold. If the signal strength of the next hop drops below the configured snr-threshold, a scan is triggered. • 2.4 GHz – Configures the snr-threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the snr-threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <-100-0> – Specify a value from -100 - 0 dB. The default is -65 dB.

```
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>	Configures the maximum tolerance period in seconds. This is the interval to wait for the root bound to recovery from a bad link. • 2.4 GHz – Configures the tolerance-period for the 2.4 GHz radio band • 5.0 GHz – Configures the tolerance-period for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <10-600> – Specify a value from 10 - 600 seconds. the default is 60 seconds.

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 osc-duration 2.4GHz 30
  acs channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands

no (meshpoint-device-config) on page 1815	Reverts the configured ACS settings to default

exclude (meshpoint-device-config)

Enables wired-peer (that are wired MiNT level-1 neighbors) exclusion

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 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 1815	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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 <-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. • <-100-0> – Specify a value from -100 - 0 dB. The default is 0 dB.
period <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. • <0-600> – Specify a value from 0 - 600 seconds. The default is 1 second.

root-sel-snr-delta <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. • <1-100> – Specify a value from 1 - 100 dB.
snr-delta <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. • <1-100> – Specify a value from 1 - 100 dB. The default is 1 dB.

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 1815	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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: • action – Sets the action taken if a critical resource goes down or if a primary port link is lost • no-root – Changes the meshpoint to be non root (this is the action taken in case any of the above mentioned two events occur)

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 1815	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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. **Note:** 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. **Note:** 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

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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

no (meshpoint-device-config) on page 1815	Removes the configuration of preferred paths for this meshpoint device

root-select (meshpoint-device-config)

Configures this mesh-point device as the cost. root

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
root-select cost-root
```

Parameters

```
root-select cost-root
```

root-select cost-root	Configures this meshpoint device as the cost root. This is necessary for dynamic root selection process. 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 1815	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.

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

Syntax

```
root {select-method [auto-mint|auto-proximity]}
```

Parameters

```
root {select-method [auto-mint|auto-proximity]}
```

root	Configures this meshpoint device as the root meshpoint
select-method auto-mint]	Optional. Enables dynamic mesh selection. When enabled, this option overrides root or no-root configuration and chooses the selection method. • auto-mint – Enables dynamic root selection using Auto-MiNT (based on path cost) The Auto-Mint or Cost Method dynamically determines the root/non-root configuration of a meshpoint by: • Monitoring and ranking the signal strength and path cost of neighboring mesh points. • Setting the configuration to: • non-root: If the link with the shortest path to the cost-root mesh device is a MCX meshpoint link • root: If the link with the shortest path to the cost-root mesh device is a non MCX meshpoint link (wired link). • This requires that the meshpoint device, in the brain car, be configured as the 'cost root' and the 'cost root' meshpoint-device be the l2 gateway to the controller. Use the root-select > cost-root command to configure a meshpoint-device as 'cost-root'. • Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root. • Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root
select-method auto-proximity	Enables dynamic root selection using meshpoint proximity. When auto-proximity 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

no (meshpoint-device-config) on page 1815	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

Configured on WiNG 7.1.X controller and pushed to the following WiNG 5.9.X APs:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8543, AP8533

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)#
```

28 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 76: Passpoint-Policy Config Mode Commands

Command	Description
3gpp on page 1818	Configures a 3gpp *(3rd Generation Partnership Project)* PLMN *(Public Land Mobile Network)* ID
access-network-type on page 1819	Configures the access network type element in this hotspot
connection-capability on page 1820	Configures the connection capability element in this passpoint policy
domain-name on page 1822	Configures the RF Domains to which this hotspot is applicable
hessid on page 1822	Configures the HESSID *(Homogeneous Extended Service Set Identifier)* for a specified hotspot zone
internet on page 1823	Advertises the availability of Internet access in this hotspot
ip-address-type on page 1824	Advertises the IP address type used in this hotspot.
nai-realm on page 1825	Configures a NAI *(Network Access Identifier)* realm name and enters its configuration mode
net-auth-type on page 1828	Configures the network authentication type used in this hotspot
operator on page 1829	Configures the operator friendly name for this hotspot
osu on page 1830	Configures an OSU *(online sign up)* SSID/provider and enters its configuration mode
roam-consortium on page 1838	Configures the list of Roaming Consortium OIs *(Organization Identifiers)* supported on this hotspot
venue on page 1839	Configures the venue group and type for this passpoint policy
wan-metrics on page 1843	Configures the WAN performance metrics for this hotspot
no on page 1844	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 on page 616 .

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)*. Note: 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

```
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: • chargeable-public – The network type is a chargeable public network. • emergency-services – The network is used to provide emergency services only. • experimental – The network is used for test or experimental purposes only. • free-public – The network type is a free public. • personal-device – The network is used for personal devices only. • private – The network is a private network. • private-guest – The network is a private network with guest access (default setting), • wildcard – Includes all access network types. 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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> [closed|open|unknown	After specifying the protocol type, specify the port (associated with the selected protocol) and its status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known Note: 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.

```
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 <0-255>	Identifies the IP protocol by the protocol's number. For example, for SMP *(simple message protocol)* specify 121.
port <0-65535> [closed|open|unknown]	After specifying the IP protocol type, specify the port number. • port <0-65535> – Select a port for the IP protocol identified. After specifying the port number, specify the port status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known Note: 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.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
internet
```

Parameters

```
None
```

Examples

```
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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]
```

ip-address-type ipv4	Configures the IPv4 address type availability information
double-nat	Specifies double NATed private IPv4 address is available
not-available	Specifies IPv4 address is not available
port-restricted	Specifies port-restricted IPV4 address is available
port-restricted-double-nat	Specifies port-restricted IPv4 address and double NATed IPv4 address is available
port-restricted-single-nat	Specifies port-restricted IPv4 address and single NATed IPv4 address is available
public	Specifies public IPv4 address is available
single-nat	Specifies single NATed IPv4 address is available
unknown	Specifies no information configured regarding the IPv4 address availability

```
ip-address-type ipv6 [available|not-available|unknown]
```

ip-address-type ipv6	Configures the IPv6 address type availability information
available	Specifies IPv6 address is available
not-available	Specifies IPv6 address is not available
unknown	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 hotpsot 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
nai-realm <NAI-REALM-NAME>
```

Parameters

```
nai-realm <NAI-REALM-NAME>
```

nai-realm <NAI-REALM-NAME>	Configures the NAI realm name for this passpoint policy • <NAI-REALM-NAME> – Specify the NAI realm name (32 characters maximum) for this passpoint policy. You can provide multiple names delimited by a semi colon.

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 77: NAI-Realm-Config-Mode Commands

Command	Description
eap-method	Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy.

Related Commands

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <1-10>	Selects the EAP authentication method used and assigns it an index number • <1-10> – 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. 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).
<1-255>	Identifies the EAP authentication method type from the corresponding IANA *(Internet Assigned Numbers Authority* number • <1-255> – Specify the IANA identity number for the authentication protocol from 1 -255.
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]	The following parameters are common to all the above authentication parameters: • cert – Certificate • hw-token – Hardware token • nfc-secure-elem – NFC secure element • none – No credential • sim – Subscriber identity module • soft-token – Soft token • username-password – Username and password • usim – Universal subscriber identity module • vendor – Vendor specific credential If setting the authentication type to either **non-eap-inner**, **inner-eap**, **credential**, or **tunneleap-credential**, define an authentication value that must be shared with the EAP credential validation server resource. If setting the authentication type to either **expanded-eap** or **expanded-inner-eap**, 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. If required, enter a 2 - 510 character vendor-specific authentication data required for the selected authentication type. Enter the value in the a-FA -F0-9 format. Provide an authentication vendor type, used exclusively for the **expanded-eap** or **expanded-inner-eap** authentication types. The vendor type must be 8 characters in length.

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 — AP505i, AP510i/e, AP560i/h

- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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: **accept-terms**, **dns-redirect**, **http-redirect**, and **online-enroll**.
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 or 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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]
```

name <OPERATOR-NAME>	Configures the operator's name in English • <OPERATOR-NAME> – Specify the operator name in ASCII format. The name cannot exceed 252 characters.
iso-lang <ISO-639-LANG-CODE> <OPERATOR-NAME>	Configures the operator's name in any language other than English • iso-lang <ISO-639-LANG-CODE> – Specify the three-character ISO-14962-1997 encoded string defining the language used in the Code field. For example, chi or spa. • <OPERATOR-NAME> – Specify the operator name in Hexadecimal format. The name cannot exceed 252 characters.

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <PASSPOINT-OSU-PROVIDER> – Specify an identification for this OSU passpoint provider serving as an online sign up identifier. Should not exceed 32 characters.
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. • <SSID> – Specify the SSID.

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 78:

Command	Description
description (osu-config-mode) on page 1832	Configures the OSU provider's description
icon (osu-config-mode) on page 1833	Adds the OSU provider's icon
method (osu-config-mode) on page 1834	Configures the open sign up methods available on this OSU provider
nai (osu-config-mode) on page 1835	Configures the OSU provider's NAI
name (osu-config-mode) on page 1835	Configures the OSU provider's name
server-url (osu-config-mode) on page 1836	Configures the OSU provider server's URL
no (osu-config-mode) on page 1837	Removes the settings configured for this OSU provider

Related Commands

no on page 1844	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <DESCRIPTION> – Specify the description. By default the system configures the name in English. Note: If configuring description in any language other than English, use the 'iso-lang' option to provide the language code.
iso-lang <ISO-LANG-CODE> <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. • <DESCRIPTION> – Specify the description in hexadecimal code.

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

no (osu-config-mode) on page 1837	Removes this OSU provider's description

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>]
```

icon iso-lang <ISO-LANG-CODE>	Configures an icon representing the OSU provider • iso-lang <ISO-LANG-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.
width <0-65535>	Configures the icon's width in pixels • <0-65535> – Specify a value from 0 - 65535 pixels.
height <0-65535>	Configures the icon's height in pixels • <0-65535> – Specify a value from 0 - 65535 pixels.
mime-type <FILE-MIME-TYPE>	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. • <FILE-MIME-TYPE> – Specify the icon's mime type.
file [<IMAGE-FILE-NAME/PATH>|<FILE-NAME>]	Configures the location and name of the image file • <IMAGE-FILE-NAME/PATH> – Specify the path and filename (255 character maximum). For example, flash:/icon.png • <FILE-NAME> – Use this option to specify the filename in the flash:/ directory

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

no (osu-config-mode) on page 1837	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
method [oma-dm|soap-xml-spp] priority <1-2>
```

Parameters

```
method [oma-dm|soap-xml-spp] priority <1-2>
```

method [oma-dm|soap-xml-spp] priority <1-2>	Configures the online sign up methods supported by this OSU provider • oma-dm – oma-dm – 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. • soap-xml-spp – 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. • priority <1-2> – Sets the priority of the specified method. Select a value from 1 - 2. The default is one (1).

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

no (osu-config-mode) on page 1837	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
nai <WORD>
```

Parameters

```
nai <WORD>
```

nai <WORD>	Configures the OSU provider's NAI • <WORD> – 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.

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) on page 1837	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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. • <NAME> – Specify the name in ASCII format. By default the system configures the name in English.
iso-lang <ISO-LANG-CODE> <NAME>	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 name in any language other than English, specify the ISO language code. • <NAME> – Specify the name in hexadecimal code.

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

no (osu-config-mode) on page 1837	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
server-url <URL>
```

Parameters

```
server-url <URL>
```

server-url <URL>	Configures the OSU provider server's URL • <URL> – Specify the server's url. Should not exceed 255 characters.

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

no (osu-config-mode) on page 1837	Removes this OSU provider's server's URL

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

no <PARAMETERS>	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)
hex <WORD>	Configures a hexadecimal input • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 type	Configures the venue group as assembly (1). This hotspot type is applicable to public assembly venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • amphitheater – Specifies the venue type as amphitheater (4) • amusement-park – Specifies the venue type as amusement park (5) • arena – Specifies the venue type as arena (1) • bar – Specifies the venue type as bar (12) • coffee-shop – Specifies the venue type as a coffee shop (13) • convention-centre – Specifies the venue type as a convention center (7) • emergency-coordination-center – Specifies the venue type as a emergency coordination center (15) • library – Specifies the venue type as a library (8) • museum – Specifies the venue type as a museum (9) • passenger-terminal – Specifies the venue type as a passenger terminal (3) • place-of-worship – Specifies the venue type as a place of worship (6) • restaurant – Specifies the venue type as a restaurant (10) • stadium – Specifies the venue type as a stadium (2) • theater – Specifies the venue type as a theater (11) • unspecified – Specifies the venue type as not specified (0) • zoo – Specifies the venue type as a zoo (14)
business type	Configures the venue group as business (2). This hotspot type is applicable to business venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • attorney – Specifies the venue type as the attorney's office (9) • bank – Specifies the venue type as a bank (2) • doctor – Specifies the venue type as a doctor or dentist's office (1) • fire-station – Specifies the venue type as a fire station (3) • police-station – Specifies the venue type as a police station (4) • post-office – Specifies the venue type as a post office (5) • professional-office – Specifies the venue type as a professional office (7) • research-and-development-facility – Specifies the venue type as a research facility (8) • unspecified – Specifies the venue type as not specified (0)
educational	Configures the venue group as educational (3). This hotspot type is applicable to educational institutions. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • school-primary – Specifies the venue type as a primary school (1) • school-secondary – Specifies the venue type as a secondary school (2) • university – Specifies the venue type as a university or college (3) • unspecified – Specifies the venue type as not specified (0)

industrial	Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • factory – Specifies the venue type as a factory (1)
	  • unspecified – Specifies the venue type as not specified (0)

institutional	Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • group-home – Specifies the venue type as a group-home (4)
	  • hospital – Specifies the venue type as a hospital (1)
	  • long-term-care – Specifies the venue type as a long term care facility (2)
	  • prison – Specifies the venue type as a prison or jail (5)
	  • rehab – Specifies the venue type as a rehabilitation facility (3)
	  • unspecified – Specifies the venue type as not specified (0)

mercantile	Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • automotive – Specifies the venue type as a automotive service center (3)
	  • gas-station – Specifies the venue type as a gas station (5)
	  • grocery – Specifies the venue type as a grocery store (2)
	  • mall – Specifies the venue type as a shopping mall (4)
	  • retail – Specifies the venue type as a retail store (1)
	  • unspecified – Specifies the venue type as not specified (0)

outdoor	Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • bus-stop – Specifies the venue type as a bus stop (5)
	  • city-park – Specifies the venue type as a city park (2)
	  • kiosk – Specifies the venue type as a kiosk (6)
	  • muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1)
	  • rest-area – Specifies the venue type as a rest area (3)
	  • traffic-control – Specifies the venue type as a traffic control area (4)
	  • unspecified – Specifies the venue type as not specified (0)

residential	Configures the venue group as residential (7). This hotspot type is applicable to residential complexes.
	• type – Specifies the venue type for this group. The options are:
	  • <0-255> – Specifies an unlisted venue type number from 0 -255
	  • boarding-house – Specifies the venue type as a boarding-house (4)
	  • dorm – Specifies the venue type as a dormitory (3)
	  • hotel – Specifies the venue type as a hotel or motel (2)
	  • private – Specifies the venue type as a private residence (1)
	  • unspecified – Specifies the venue type as not specified (0)

storage	Configures the venue group as storage (8). This hotspot type is applicable to storage groups. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
unspecified	Configures the venue group as unspecified (0) • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
utility-and-misc	Configures the venue group as utility and miscellaneous (8) • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
vehicular	Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • airplane – Specifies the venue type as an airplane (2) • auto – Specifies the venue type as an automobile or truck (1) • bus – Specifies the venue type as a bus (3) • ferry – Specifies the venue type as a ferry (5) • motor-bike – Specifies the venue type as a motor bike (7) • ship – Specifies the venue type as a ship or boat (5) • train – Specifies the venue type as a train (6) • unspecified – Specifies the venue type as not specified (0)

```
operator name <VENUE-NAME>
```

name <WORD>	Configures the venue name in English • <WORD> – Specify the venue name in ASCII format.

```
operator name iso-lang <ISO-LANG-CODE> <VENUE-NAME>
```

name iso-lang <ISO-LANG-CODE> <VENUE-NAME>	Configures a non-English venue name • iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). • <ISO-LANG-CODE> – Specify the 3 character iso-639 language code. <VENUE-NAME> – Specify the venue name as a hexadecimal code,

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

no	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps.
up-speed <0-4294967295>	Configures the up stream traffic speed • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps.

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

no	Removes the WAN metrics configuration on this passpoint policy

no

Removes or reverts the passpoint policy settings

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>
```

no <PARAMETERS>	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)#
```

29 Crypto-CMP Policy

crypto-cmp-policy-instance
other-cmp-related-commands

This chapter summarizes the crypto *certificate management protocol* (CMP) 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 *Public Key Infrastructure* (PKI) network. A *Certificate Authority* (CA) 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 79: Crypto-CMP-Policy Config Mode Commands

Description	Command
ca-server	Configures the CA server details
cert-key-size on page 1848	Configures the size of the key associated with a certificate request
cert-renewal-timeout on page 1849	Configures a certificate renewal timeout in days
cross-cert-validate on page 1850	Enables validation of the cross certificate with the factory certificate
hash-algorithm on page 1851	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.
subjectAltName on page 1851	Configures an alternate subject name for this CMP policy
trustpoint on page 1852	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
use on page 1854	Associates a device's autogen-uniqueid with this crypto CMP policy
no on page 1855	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 on page 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 [primary| secondary]	Configures the primary and secondary CMP CA server details (IPv4 address, port, and path) • primary – Configures the primary CMP CA server's details • secondary – Configures the secondary CMP CA server's details The secondary CMP CA is used in case the primary CA server is not reachable. CA server settings are required to complete CMP requests.
host <IP>	Configures IP address or hostname of the device hosting the CA server • <IP/HOSTANAME> – Specify the IP address or hostname.
port <PORT-NUMBER>	Configures IPv4 address of the device hosting the primary/secondary CA server • <IP/HOSTNAME> – Specify the server's IPv4 address.
port <1-65535>	Configures the port on which the primary/secondary CA server can be reached • <1-65535> – Specify the port number from 1 - 65535.
path <PATH>	Configures the path or filename of the primary/secondary CMP CA certificate. Enter the complete relative path to the file on the server. • <PATH> – Specify the path. Once specified, the certificate is downloaded from this location and installed on the device.

Examples

```
ap505-D8273A(config-cmp-policy-CMP)#ca-server primary host 192.168.8.74 port 8 path cmp
ap505-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
ca-server primary host 192.168.8.74 port 80 path cmp
ap505-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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cert-key-size [2048|3072|4096]
```

Parameters


```
cert-key-size [2048|3072|4096]
```


cert-key-size [2048|3072|4096]	Configures the certificate request key size. The options are: • 2048 – Sets the key size to 2048 bits. This is the default setting. • 3072 – Sets the key size to 3072 bits • 4096 – Sets the key size to 4096 bits

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

no on page 1855	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
cert-renewal-timeout <1-60>
```

Parameters


```
cert-renewal-timeout <1-60>
```

cert-renewal-timeout <1-60>	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. • <1-60> – 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.

Examples

```
ap505-D8273A(config-cmp-policy-CMP)#cert-renewal-timeout 60

ap505-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
ap505-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no on page 1855	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 1300.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1855	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
hash-algorithm [sha1|sha256|sha384|sha512]
```

Parameters

```
hash-algorithm [sha1|sha256|sha384|sha512]
```

hash-algorithm [sha1|sha256|sha384|sha512]	Configures the hashing algorithm type. The options are: • sha1 – Uses SHA1 *(Secure Hash Algorithm 1)* hash function. This is the default setting. • sha256 – Uses SHA256 hash function. • sha384 – Uses SHA384 hash function. • sha512 – Uses SHA512 hash function. Note: The **sha256**, **sha384** and **sha512** hash functions belong to the SHA-2 family of algorithms.

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 1855	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-D8273A(config-cmp-policy-CMP)#subjectAltName dn TechPubsCA
ap505-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
ap505-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no on page 1855	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 <TRUSTPOINT-NAME>	Configures a trustpoint name (should not exceed 32 characters) • <TRUSTPOINT-NAME> – Specify the trustpoint's name.
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. • 0 <WORD> – Configures a clear text password • 2 <WORD> – Configures an encrypted password • <WORD> – Specify the password.
reference-id <WORD>	Configures the reference ID. The CA server uses this information to identify the shared secret key used. • <WORD> – Specify the reference ID.
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. • <WORD> – Specify the sender name.
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 • <CERT-PATH> – Specify the certificate path.

Examples

```
ap505-D8273A(config-cmp-policy-CMP)#trustpoint cmp-test subject-name "CN=Examp
leCompany, O=Example Company" secret 0 test-secret reference-id 123456 sender-na
me "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company,
 CN=ExampleCompany.com"
ap505-D8273A(config-cmp-policy-CMP)#

ap505-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
ap505-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	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 880.

Supported in the following platforms:

- Access Points — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-D8273A(config-cmp-policy-CMP)#use autogen-uniqueid
ap505-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
ap505-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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

```
ap505-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
ap505-D8273A(config-cmp-policy-CMP)#

ap505-D8273A(config-cmp-policy-CMP)#no cert-renewal-timeout

ap505-D8273A(config-cmp-policy-CMP)#no subjectAltName

ap505-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"
ap505-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 80: Other-CMP-Related Commands

Command	Description
use (other-cmp-related-commands) on page 1856	Associates a crypto CMP policy with a device
show (other-cmp-related-commands) on page 1856	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

Parameters

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

cmp-policy <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. • <CRYPTO-CMP-POLICY-NAME> – Specify the crypto CMP policy name. Should be existing and configured.

Examples

```
ap505-D8273A(config-device-00-11-3F-D8-27-3A)#use crypto-cmp-policy CMP
ap505-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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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>}	Displays the current status of all on-going CMP requests • on <DEVICE-NAME> – Optional. Optionally specify the name of the AP, wireless controller, or service platform to view CMP request status on a specified device.

```
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}
```

show pki trustpoints {<TRUSTPOINT-NAME>|all} on <DEVICE-NAME>	Displays all trustpoints including CMP generated trustpoints • <TRUSTPOINT-NAME> – Optional. Specify a trustpoint name. Displays details of the trustpoint identified by the <TRUSTPOINT-NAME> parameter. • all – Optional. Displays details of all configured trustpoints • on <DEVICE-NAME> – Optional. Specify the name of the AP, wireless controller, or service platform to view trustpoints configured on a specified device.

Examples

```
ap505-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
-------------------------------------------------------------------------------------

ap505-D8273A#
ap505-D8273A(config)#show crypto cmp request status
CMP Request Status:   cmp-complete

ap505-D8273A#
```

30 Roaming Assist Policy

roaming-assist-policy commands

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
action on page 1859	Specifies the action to be invoked on the client
aggressiveness on page 1860	Configures a roaming aggressiveness value for wireless clients
detection-threshold on page 1861	Configure detection-threshold interval value
disassoc-time on page 1862	Configures the disassociation interval
handoff-count on page 1862	Configures the handoff-count value
handoff-threshold on page 1863	Configures the handoff-threshold value
monitoring-interval on page 1864	Configures the client monitoring interval
sampling interval on page 1865	Configures the interval at which clients are sampled to determine their RSSI value
no on page 1865	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 on page 616.

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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
action [assisted-roam|deauth|log]
```

Parameters

```
action [assisted-roam|deauth|log]
```

action [assisted-roam|deauth|log]	Configures the action invoked on the client once it reaches the specified threshold value. The options are: • assisted-roam – Provides 802.11v assisted roaming facility to the client • deauth – De-authenticates the client. This is the default setting. • log – Generates a log Note: In all three cases an event is generated. However, the message generated differs and is based on the action specified.

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 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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

no on page 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
disassoc-time <1-10>
```

Parameters

```
disassoc-time <1-10>
```

disassoc-time <1-10>	Configures the disassociation time in seconds • <1-10> – Specify a value from 1 - 10 seconds. The default is 5 seconds.

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

no on page 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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 • <1-10> – Specify a value from 1 - 10. The default is 3. 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

no on page 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
handoff-threshold <-100--40>
```

Parameters

```
handoff-threshold <-100--40>
```

handoff-threshold <-100--40>	Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked. • <-100--40> – Specify the RSSI value from -100 dBm - -40 dBm. The default is -80 dBm. 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-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 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
monitoring-interval <1-60>
```

Parameters

```
monitoring-interval <1-60>
```

monitoring-interval <1-60>	Specifies the interval, in seconds, at which clients are monitored to determine if their RSSI is below the specified handoff-threshold • <1-60> – Specify the duration from 1 - 60 seconds. The default is 5 seconds.

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

no on page 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

Syntax

```
sampling-interval <5-60>
```

Parameters

```
sampling-interval <5-60>
```

sampling-interval <5-60>	Configures the interval, in seconds, between two successive client samplings • <5-60> – Specify a value from 5 - 60 seconds. The default value is 15 seconds. **Note:** 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

no on page 1865	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 — AP505i, AP510i/e, AP560i/h
- Service Platforms — NX5500, NX7500, NX9500, NX9600, VX9000

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)#
```

31 Border Gateway Protocol

bgp ip-prefix-list
bgp ip-access-list
bgp as-path-list
bgp community-list
bop ext-community-list
bgp route-map
bgp router-config
bgp neighbor-config

This chapter summarizes the *Border Gateway Protocol* (BGP) 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 *Autonomous Systems* (ASs) 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: *external BGP* (eBGP) and *internal BGP* (iBGP). 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 81: BGP IP-Prefix-List Config Mode Commands

Command	Description
deny (ip-prefix-list) on page 1869	Creates and configures a deny, prefix-list rule
permit (ip-prefix-list) on page 1870	Creates and configures a permit, prefix-list rule
no (ip-prefix-list) on page 1871	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]
```

deny prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]	Creates and configures a deny prefix-list rule • <1-4294967295> – 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. • <PREFIX-TO-MATCH/MASK> – 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. ge <0-32> – Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask) le <0-32> – Optional. Specifies a less than or equal to value for the IP prefix length The 'ge' and 'le' options specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria. 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.

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

no (ip-prefix-list) on page 1871	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]
```

deny prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]	Creates and configures a permit prefix-list rule • <1-4294967295> – 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. • <PREFIX-TO-MATCH/MASK> – 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. ge – Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask) le – Optional. Specifies a less than or equal to value for the IP prefix length 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. • 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.

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

no (ip-prefix-list) on page 1871	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 82: BGP IP-Access-List Config Mode Commands

Command	Description
deny (bgp-ip-access-list) on page 1872	Creates and configures a deny entry rule for this BGP IP ACL
permit (bgp-ip-access-list) on page 1873	Creates and configures a permit entry for this BGP IP ACL
no (bgp-ip-acess-list) on page 1874	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]
```

deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}| any]	Creates and configures a deny entry for this BGP IP ACL • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. • exact-match – 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. • any – Specifies the prefix to match as 'any'.

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

no (bgp-ip-acess-list) on page 1874	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 • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. • 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. • any – Specifies the prefix to match as 'any'.

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

no (bgp-ip-acess-list) on page 1874	Removes the specified the permit entry in this IP BGP ACL

no (bgp-ip-acess-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 83: BGP AS-Path-List Config Mode Commands

Command	Description
deny (bgp-as-path-list) on page 1875	Creates and configures a deny as-path-list rule
permit (bgp-as-path-list) on page 1876	Creates and configures a permit as-path-list rule
no (bgp-as-path-list) on page 1877	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). • <REG-EXP> – Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule) 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 84:

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

no (bgp-as-path-list) on page 1877	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). • <REG-EXP> – Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule) 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 85:

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

no (bgp-as-path-list) on page 1877	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>
```

no <PARAMETERS>	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 86: BGP Community-List Config Mode Commands

Command	Description
deny (bgp-community-list) on page 1879	Creates and configures a deny community (expanded or standard) rule
permit (bgp-community-list) on page 1880	Creates and configures a permit community (expanded or standard) rule
no (bgp-community-list) on page 1882	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>
```

`deny community expanded <LINE>`	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. • <LINE> – Provide the regular expression.

```
deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

deny community standard [AA:NN| internet| local-AS|no-advertise| no-export]	Configures a deny standard community list entry and associates it with a predefined, globally used, known community or community number. The options are: • aa:nn - Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number. • internet – Advertises this route to the internet community • local-AS – Prevents transmission of this route outside the local AS • no-advertise – Prevents advertisement of this route to any peer (internal or external • no-export – Prevents advertisement of this route to external BGP peers (keeping this route within an AS)

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

no (bgp-community-list) on page 1882	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>
```

`permit community expanded <LINE>`	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. • <LINE> – Provide the regular expression.

```
permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

permit community standard [AA:NN|internet| local-AS| no-advertise| no-export]	Configures a permit standard community list entry and associates it with a predefined, globally used, known community or community number. The options are: • aa:nn - Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number. • internet – Advertises this route to the internet community • local-AS – Allows transmission of this route outside the local AS • no-advertise – Allows advertisement of this route to any peer (internal or external • no-export – Allows advertisement of this route to external BGP peers (keeping this route within an AS)

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

no (bgp-community-list) on page 1882	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>
```

no <PARAMETERS>	Removes a deny or permit expanded community rule from this community list • <LINE> – Specify the regular expression associated with the rule.

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 an 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-excommunity-list-<EXTCOMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP extended community list configuration commands:

Table 87: BGP-Ext-Community-List Config Mode Commands

Command	Description
deny (bgp-ext-community-list) on page 1883	Creates and configures a deny extended community (expanded or standard) rule
permit (bgp-ext-community-list) on page 1884	Creates and configures a permit extended community (expanded or standard) rule
no (bgp-ext-community-list) on page 1885	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>
```

deny extcommunity expanded <LINE>	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. • <LINE> – Provide the regular expression.

```
deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>	Configures a deny standard named extended community list entry. and associates it with the target or origin community attributes. • rt – Configures the RT *(route target)* extended community attribute • soo – Configures the SOO *(site-of-origin)* extended community attribute <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)#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

no (bgp-ext-community-list) on page 1885	Removes the specified deny extended community rule from this extcommunity list

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. • <LINE> – Provide the regular expression.

```
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. • rt – Configures the RT extended community attribute • soo – Configures the SOO extended community attribute <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 1885	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 88: BGP-Route-Map Config Mode Commands

Command	Description
description (bgp-route-map) on page 1887	Configures a description for this route-map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions
match (bgp-route-map) on page 1888	Configures the match criteria associated with this deny or permit BGP route map
set (bgp-route-map) on page 1891	Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules
no (bgp-route-map) on page 1895	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

no (bgp-route-map) on page 1895	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 An AS path is a list of ASs a packet traverses to reach its destination. • <AS-PATH-LIST-NAME> – Specify the AS path list name (should be existing and configured)
community <COMMUNITY-LIST-NAME> {exact-match}	Configures the AS community list string to match • <COMMUNITY-LIST-NAME> – Specify the AS community list name (should be existing and configured). • exact-match – Optional. Does an exact match when matching the specified AS community string. This option is disabled by default.
extcommunity <EXTCOMMUNITY-LIST-NAME>	Configures the external community list string to match • <EXTCOMMUNITY-LIST-NAME> – Specify the external community list name (should be existing and configured).

```
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 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: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – 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).

ip-next-hop [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>| prefix-list <PREFIX-LIST-NAME>]	Configures the next-hop's IP address to match 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: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – 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).
ip-route-source [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>| prefix-list <PREFIX-LIST-NAME>]	Configures the advertised route source IP address to match 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: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – 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).

```
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 Filter List_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 1895	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>
```

set aggregator-as <1-4294967295> <IP>	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. • <1-4294967295> – Specify the route aggregator's ASN from 1-4294967295. This option is disabled by default. • <IP> – Specify the route aggregator's IP address. BGP allows the aggregation of specific routes into one route using an aggregate IP address.

```
set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}
```

set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}	Configures the BGP transform AS path attribute to be applied to filtered routes • exclude – Configures a single AS, or a list of ASs, excluded from the AS path • prepend – Configures a single AS, or a list of ASs, prepended to the AS path • <1-4294967295> – 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. You can configure multiple ASNs.

```
set atomic-aggregate
```

set atomic-aggregate	Enables BGP atomic aggregate attributes 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.

```
set comm-list delete <COMMUNITY-LIST-NAME>
```

set comm-list delete <COMMUNITY-LIST-NAME>	Deletes specified BGP communities. All communities matching the community list name string are deleted from the route. A BGP community is a group of routes sharing a common attribute. • <COMMUNITY-LIST-NAME> – Specify the community list name.

```
set community [<COMMUNITY-NUMBER>|none]
```

set community [<COMMUNITY-NUMBER>|none]	Configures a community attribute for this route
	• <COMMUNITY-NUMBER> – Specify a community attribute. Use one of the following formats:
	  • internet - Advertises this route to the Internet. This is a global community.
	  • local-AS - Prevents the transmit of packets outside the local AS
	  • no-advertise - Prevents advertisement of this route to any peer, either internal or external
	  • no-export - Prevents advertisement of this route to BGP peers, keeping this route within an AS.
	  • aa:nn - Configures the first part (aa) representing the AS number. The second part (nn) represents a 2-byte number.
	• none – Specifies community attribute as none

```
set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>
```

set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>	Configures a extended community attribute for this route • rt – Identifies the route target (rt) extended community • soo – Identifies the site-of-origin (soo) community. This is the origin community associated with the route reflector. • <EXTCOMMUNITY-NUMBER> – This keyword is common to the 'rt' and 'soo' parameters. Use it to specify the extended community number.

```
set ip next-hop [<IP>|peer-address]
```

set ip next-hop [<IP>|peer-address]	Configures the next hop for this route. Use one of the following options to identify the next hop: • <IP> – Specify the nest hop's IP address • peer-address – Enables the identification of the next-hop address for peer devices. This option is disabled by default

```
set local-preference <0-4294967295>
```

set local-preference <0-4294967295>	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. • <0-4294967295> – Specify the preference value from 0 - 4294967295.

```
set metric <0-4294967295>
```

set metric <0-4294967295>	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. • <0-4294967295> – Specify the metric from 0 - 4294967295.

```
set origin [egp|igp|incomplete]
```

set origin [egp|igp|incomplete]	Configures the origin code for this BGP route map • egp - Sets the origin of the route to eBGP • igp - Sets the origin of the route to iBGP • 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.

```
set originatorid <IP>
```

set originatorid <IP>	Configures this route map's originator IP address

```
set source-ip <IP>
```

set source-ip <IP>	Configures this route map's source IP address • <IP> – Specify the IP address in the A.B.C.D format.

```
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. • <0-65335> – 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 1895	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 89: BGP-Router Config Mode Commands

Command	Description
aggregate (bgp-router-config) on page 1898	Creates and configures an aggregate address entry in the BGP database
asn (bgp-router-config) on page 1899	Configures this BGP router's ASN
bgp (bgp-router-config) on page 1899	Configures BGP router parameters

Table 89: BGP-Router Config Mode Commands (continued)

Command	Description
bgp-route-limit (bgp-router-config) on page 1904	Configures the BGP route limit parameters
distance (bgp-router-config) on page 1905	Configures administrative distance parameters
ip (bgp-router-config) on page 1906	Configures the BGP default gateway's priority
network (bgp-router-config) on page 1907	Configures the local network IP addresses and masks
route-redistribute (bgp-router-config) on page 1908	Enables redistribution of routes learnt from other routing protocols into BGP
timers (bgp-router-config) on page 1910	Enables adjustment of keepalive and holdtime intervals
no (bgp-router-config) on page 1911	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 • summary-only – Optional. Filters more specific routes from updates

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

no (bgp-router-config) on page 1911	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>
```

asn <1-4294967295>	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

no (bgp-router-config) on page 1911	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. 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 *deterministic-med* option.
deterministic-med	Enables selection of the best MED path from amongst all paths advertised by neighboring ASs. This option is disabled by default. 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	Enables immediate resetting of BGP session on the interface once the BGP connection goes down. This option is enabled by default. 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. To configure the 'holdtime', use the **timers > bgp > <keepalive-time> > <holdtime>** command in this (BGP router) configuration mode.
log-neighbor-changes	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.

```
bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}|
missing-as-worst}]
```

best-path	Modifies the bestpath selection algorithm. The route selection algorithm uses the following criteria when selecting the preferred route: as-path, router-id, and med.
as-path [confed|ignore]	Enables an AS path from being considered as a criteria for selecting the preferred route • confed – Enables comparison of path lengths (including confederation sets and sequences) when selecting a route (EXPERIMENTAL). This option is disabled by default. • 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.
compare-router-id	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.
med {confed {missing-as-worst}| missing-as-worst}	Enables comparison of AS path MED value when selecting the preferred route 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. • 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. • 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.

```
bgp client-to-client reflection
```

client-to-client reflection	Enables client-to-client route reflection (EXPERIMENTAL) 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.

```
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. • <0-4294967295> – Specify a value from 10 - 4294967295.

```
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 • stalepath-time <1-3600> – 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. • <1-3600> – Specify a value from 1 - 3600 seconds.

```
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. • <IP> – Specify the IP address in the A.B.C.D format. For BGP neighbor configuration parameters, see bgp-neighbor-config commands.

```
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-bgpp)#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 1911	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. • <1-32> – Specify a value from 1 - 32. The default is 5 routes.
retry-timeout <1-3600>	Configures the duration, in seconds, the BGP process is temporarily shut down, before a reset of the process is attempted. • <1-3600> – Specify a value from 1 - 3600 seconds. The default is 60 seconds.

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

no (bgp-router-config) on page 1911	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>	Configures the default administrative distance, specified by the • <1-255> parameter, when the route's source IP address matches the specified IP prefix • <IP/M> – Specify the IP source prefix and prefix length. <1-255> – Specify the distance from 1 - 255. <BGP-ACL-NAME> – Optional. Specify the BGP access list name.
bgp <1-255> <1-255> <1-255>	Configures the default administrative distance for different route types • <1-255> – Configures the default administrative distance for routes external to this AS. Specify a value from 1 - 255. • <1-255> – Configures the default administrative distance for routes internal to this AS. Specify a value from 1 - 255. <1-255> – Configures the default administrative distance for local routes. Specify a value from 1 - 255.

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 1911	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>	Configures the default gateway's (acquired through BGP) priority • <1-8000> – Specify a value from 1 - 8000. The default is 7500. Lower the value, higher is the priority.

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

no (bgp-router-config) on page 1911	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 • <IP/M> – Specify the network address.
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. • pathlimit <1-255> – Specify the hop count limit from 1 - 255.
pathlimit <1-255>	Optional. Configures the maximum path limit for this AS • <1-255> – Specify the hop count limit from 1 - 255.
route-map <ROUTE-MAP-NAME>	Optional. Associates a BGP route map with this local network. When applied, the route-map values take precedence • <ROUTE-MAP-NAME> – Specify the route map name.

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

no (bgp-router-config) on page 1911	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 • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. route-map • <ROUTE-MAP-NAME> – 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 match.
kernel	Redistributes kernel routes. These are routes that are neither connected, nor static, nor dynamic. • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – 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 match.
ospf	Redistributes OSPF routes • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – 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 match.
static	Redistributes static routes • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – 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 match.

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

no (bgp-router-config) on page 1911	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>
```

timers bgp <0-65535> <0-65535>	Configures the keepalive and holdtime interval in seconds • <0-65535> – 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. • <0-65535> – 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.

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

no (bgp-router-config) on page 1911	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>
```

no <PARAMETERS>	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 90: BGP-Neighbor Config Mode Commands

Command	Description
activate (bgp-neighbor-config) on page 1915	Enables an address family for this neighbor (EXPERIMENTAL)
advertisement-interval (bgp-neighbor-config) on page 1915	Configures the minimum interval between two consecutive BGP router updates
allowas-in (bgp-neightbor-config) on page 1916	Enables re-advertisement of all prefixes containing duplicate ASNs (EXPERIMENTAL)
attribute-unchanged (bgp-neighbor-config) on page 1917	Enables the propagation of BGP attribute values unchanged to this neighbor BGP device (EXPERIMENTAL)
capability (bgp-neighbor-config) on page 1917	Enables the advertisement of capability (dynamic and ORF) to BGP peers
default-originate (bgp-neighbor-config) on page 1918	Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route.
description (bgp-neighbor-config) on page 1919	Configures a description for a BGP neighbor device
disable-connected-check (bgp-neighbor-config) on page 1920	Enables one-hop away EBGP peer using loop back address (EXPERIMENTAL)
dont-capability-negotiate (bgp-neighbor-config) on page 1920	Disables capability negotiation with BGP neighbors (EXPERIMENTAL)
ebgp-multihop (bgp-neighbor-config) on page 1921	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.
enforce-multihop (bgp-neighbor-config) on page 1922	Forces EBGP neighbors to perform multi-hop checks (EXPERIMENTAL)
local-as (bgp-neighbor-config) on page 1922	Configures this neighbor's local AS number. Also enables the prepending of this AS number in route updates. (EXPERIMENTAL)
maximum-prefix (bgp-neighbor-config) on page 1923	Configures the maximum number of prefixes that can be received from a BGP neighbor
next-hop-self (bgp-neighbor-config) on page 1924	Enables next-hop calculation for this neighbor

Table 90: BGP-Neighbor Config Mode Commands (continued)

Command	Description
override-capability (bgp-neighbor-config) on page 1925	Enables the overriding of capability negotiation results
passive (bgp-neighbor-config) on page 1926	Enables this BGP neighbor device (or devices using this profile) as passive
password (bgp-neighbor-config) on page 1927	Sets a password for this BGP neighbor device (or devices using this profile)
peer-group (bgp-neighbor-config) on page 1928	Sets the peer group for this BGP neighbor device (or devices using this profile) (EXPERIMENTAL)
port (bgp-neighbor-config) on page 1929	Configures a non-standard BGP port for this BGP neighbor (EXPERIMENTAL)
remote-as (bgp-neighbor-config) on page 1930	Configures the ASN for this neighbor BGP device (or devices using this profile)
remove-private-as (bgp-neighbor-config) on page 1931	Removes the private ASN from outbound updates (EXPERIMENTAL)
route-server-client (bgp-neighbor-config) on page 1932	Enables this BGP neighbor device (or devices using this profile) to act as a route server client (EXPERIMENTAL)
send-community (bgp-neighbor-config) on page 1932	Enables sending of the community attribute to the BGP neighbor
shutdown (bgp-neighbor-config) on page 1933	Shuts down this BGP neighbor device (or devices using this profile)
soft-reconfiguration (bgp-neighbor-config) on page 1934	Enables storing of updates for inbound soft reconfiguration
strict-capability-match (bgp-neighbor-config) on page 1935	Enables a strict capability match before allowing a neighbor BGP peer to open a connection (EXPERIMENTAL)
timers (bgp-neighbor-config) on page 1935	Configures this BGP neighbor's keepalive and holdtime durations
unsuppress-map (bgp-neighbor-config) on page 1937	Uses a route-map that selectively un suppresses routes that have been suppressed using the aggregate-address command
update-source (bgp-neighbor-config) on page 1937	Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor
use (bgp-neighbor-config) on page 1938	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.
weight (bgp-neighbor-config) on page 1939	Configures a weight for all routes learned from this BGP neighbor
no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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. • <0-600> – Specify a value from 0 - 600 seconds. The default is 5 seconds.

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

no (bgp-neighbor-config) on page 1940	Reverts the minimum interval between two consecutive BGP router updates to default (5 seconds)

allowas-in (bgp-neightbor-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

```
allowas-in <1-10>
```

Parameters

```
allowas-in <1-10>
```

allowas-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)#allowas-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
   allowas-in 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no (bgp-neighbor-config) on page 1940	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
   allowas-in 10
   attribute-unchanged as-path
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no (bgp-neighbor-config) on page 1940	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
```

capability dynamic	Enables the advertisement of dynamic capability 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]
```

capability orf prefix-list [both|receive|send]	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 {route-map <BGP-ROUTE-MAP-NAME>}`	Enables default originate on this BGP neighbor. This option is disabled by default. • route-map <BGP-ROUTE-MAP> – Optional. Use this keyword to specify a route map to use as the default originate route. **Note:** If no route-map is specified, the default route 0.0.0.0 is sent.

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 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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}
```

local-as <1-4294967295> *{no-prepend}*	Configures the local AS number • <1-4292967295> – Specify a value from 1 - 4294967295. • 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.

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

no (bgp-neighbor-config) on page 1940	Removes the local AS number. And also reverts prepending of AS numbers to default (allows prepending).

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)}

maximum-prefix <1-4294967295>	Configures the maximum number of prefixes that can be received from a BGP neighbor • <1-4294967295> – Specify a value for 1 - 4294967295. • <1-100> – 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. • restart <1-65535> – 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. • 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.

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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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. • <PEER-GROUP-NAME> – Specify the peer group name.

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
   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 1940	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 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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]
```

send-community [both|extended|standard]	Enables sending of the community attributes to the BGP neighbor • both – Sends extended and standard community attributes • extended – Sends extended community attributes only • standard – Sends standard community attributes only

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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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 • <0-65535> – 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. • <0-65535> – 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.
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. • <0-65535> – Specify a value from 1 - 65535 seconds.

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

no (bgp-neighbor-config) on page 1940	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>
```

unsuppress-map <ROUTE-MAP-NAME>	Un-suppresses the specified route map • <ROUTE-MAP-NAME> – Specify the route map name.

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

no (bgp-neighbor-config) on page 1940	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

no (bgp-neighbor-config) on page 1940	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>]
```

`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>]`	Uses predefined and configured filters with this neighbor
	• distribute-list <BGP-IP-ACL-NAME> – Uses a BGP IP ACL
	  • <BGP-IP-ACL-NAME> – Specify the BGP IP ACL name.
	• filter-list <AS-PATH-LIST-NAME> – Uses an AS path list
	  • <AS-PATH-LIST-NAME> – Specify the AS path list name.
	• prefix-list <IP-PREFIX-LIST-NAME> – Uses a IP prefix list
	  • <IP-PREFIX-LIST-NAME> – Specify the IP prefix list name.
	• route-map <BGP-ROUTE-MAP-NAME> – Uses a route map
	  • <BGP-ROUTE-MAP-NAME> – Specify the route map name.

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

no (bgp-neighbor-config) on page 1940	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>
```

weight <0-65535>	Specifies a relative weightage for all routes learned from this neighbor • <0-65535> – Specify a value from 0 - 65535.

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

no (bgp-neighbor-config) on page 1940	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>
```

no <PARAMETER>	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)#
```

A 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 7602access 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 7602access 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 2: 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 a 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 wirless 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 1946
- Creating a AP 7602Profile on page 1947

Creating an AP 7161 Profile

Folow 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-AP7131_Us
```

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.

Folow 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 Domainto 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 the SSID of the controller-managed WLAN created and mapped to the access points.
- Click **Connect**. You should get intenet access.

B AP Dual Modes of Operation

Understanding Dual Mode Capability

Understanding Dual Mode Capability

The WiNG 7.1 AP5XX model access points have the capability of operating in the following two modes: **`Distributed`** and **`Centralized`**. For a newly-manufactured, out-of-the-box AP5XX access point the mode of operation is *not specified*. The *Centralized* mode of operation is ideally suited for dense localized deployments, while the *Distributed* mode supports scaled-out deployments.

Refer to the following sections for more information:

- Auto-discovery of AP's Mode of Operation on page 1951
- Manually-setting AP's Mode of Operation on page 1952

Auto-discovery of AP's Mode of Operation

When a newly-manufactured AP5XX access point boots up for the first time it goes through the following procedure:

1. The AP runs the discovery image to determine its mode of operation.
2. If the AP finds Distributed discovery methods, it reboots into the '*Distributed*' mode.
3. If the AP finds Centralized discovery methods, it reboots into the '*Centralized*' mode.
4. The AP then tries to discover and adopt to an adopter. The following adoption scenarios are possible for the two modes of operation:
   - AP in Distributed mode — can adopt to a WiNG VC, WiNG Controller or ExtremeCloud Appliance
   - AP in Centralized mode — can adopt to ExtremeCLoud Appliance

Note
If the AP (Centralized or Distributed) adopts to ExtremeCloud Appliance, its final mode of operation is determined by the type of site in which the AP is placed. If it is placed in a Distributed site, its mode is set to 'Distributed'. If placed in a 'Centralized site', its mode is set to 'Centralized'. For more information on ExtremeCloud Appliance adoption and configuration, please refer to the ExtremeCloud Appliance User Guide available at https://extremenetworks.com/documentation.

Note
If the AP fails to adopt to any of the above mentioned adopters, you can manually set the AP to the **`Standalone`** mode. For more information, see Manually-setting AP's Mode of Operation on page 1952.

Note
For information on how to reset the mode of operation of an AP adopted to a WiNG VC or Controller, see Resetting an AP's Mode of Operation on page 1954.

Manually-setting AP's Mode of Operation

You will need to manually set the AP's mode of operation if:

- the AP boots up for the first time and is unable to discover and adopt to any of the following adopter options: **`WiNG (VC)`**, **`WiNG Controller`**, **`ExtremeCloud Appliance`**.
- you want to deploy the AP as a **`Standalone/WiNG`** or as **`WiNG Virtual Controller`**.

You can either use the AP's CLI or GUI to set the mode of operation.

Using CLI to Set AP's Mode of Operation

To manually set the AP's mode of operation using its CLI:

1 Access the AP's CLI through SSH or console using default credentials.

Use the AP's Primary or Secondary (ZEROCONF) IP address to do an SSH.

Primary IP address - This is the DHCP provided IP address.

Secondary IP address - This is the ZEROCONF IP address '169.254. xx.yy'. Where, '`xx`' and '`yy`' are the last two octets of the AP's MAC address in decimal format. Note, the AP's MAC address will be printed on the box.

For example:

If AP's MAC address is: *00:C0:23:00:**F0:0A***

The secondary IP address will be: *169.254.**240.10***

You will be presented with the following message:

```
AP adoption discovery process in progress…
To cancel and boot in Standalone mode, type (s):
```

2 Type '`s`' to move into the '`Standalone/WiNG`' mode.

```
AP adoption discovery process in progress…
To cancel and boot in Standalone mode, type (s): s

AP booting in Standalone mode…
```

The AP will reboot immediately. After reboot, you will be presented with the WiNG login prompt.

3 Use the following default credentials to login:

username: `admin`

password: `admin123`

Using GUI to Set AP's Mode of Operation

To manually set the AP's mode of operation using its GUI:

1 Access the AP's GUI through a Web browser (http://<AP-IP-ADDRESS>).

Point the Web browser to the AP's Primary or Secondary (ZEROCONF) IP address.

Primary IP address - This is the DHCP provided IP address.

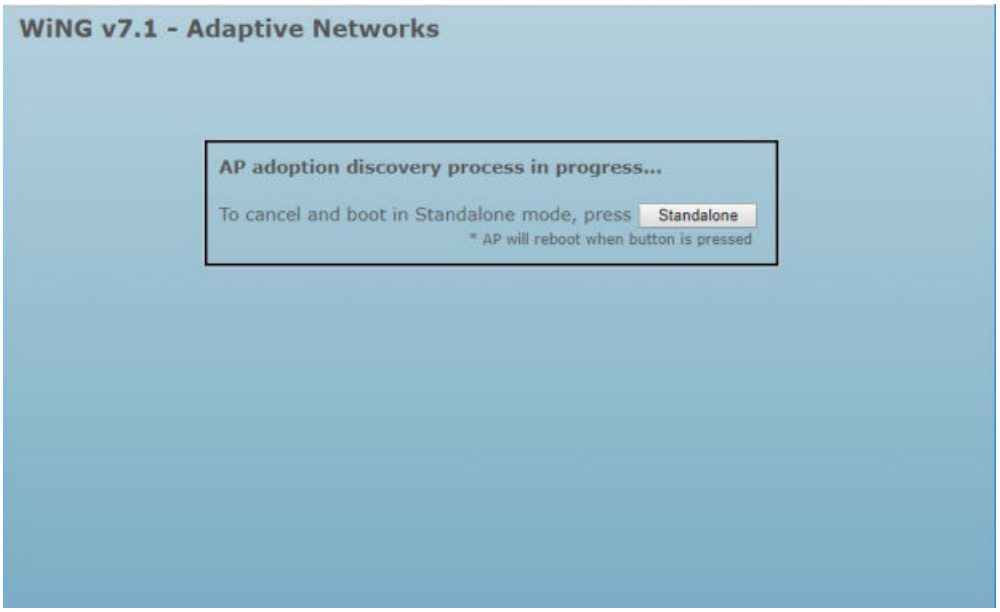
Secondary IP address - This is the ZEROCONF IP address '169.254. xx.yy'. Where, '`xx`' and '`yy`' are the last two octets of the AP's MAC address in decimal format. Note, the AP's MAC address will be printed on the box.

For example:

If AP's MAC address is: *00:C0:23:00:**F0:0A***

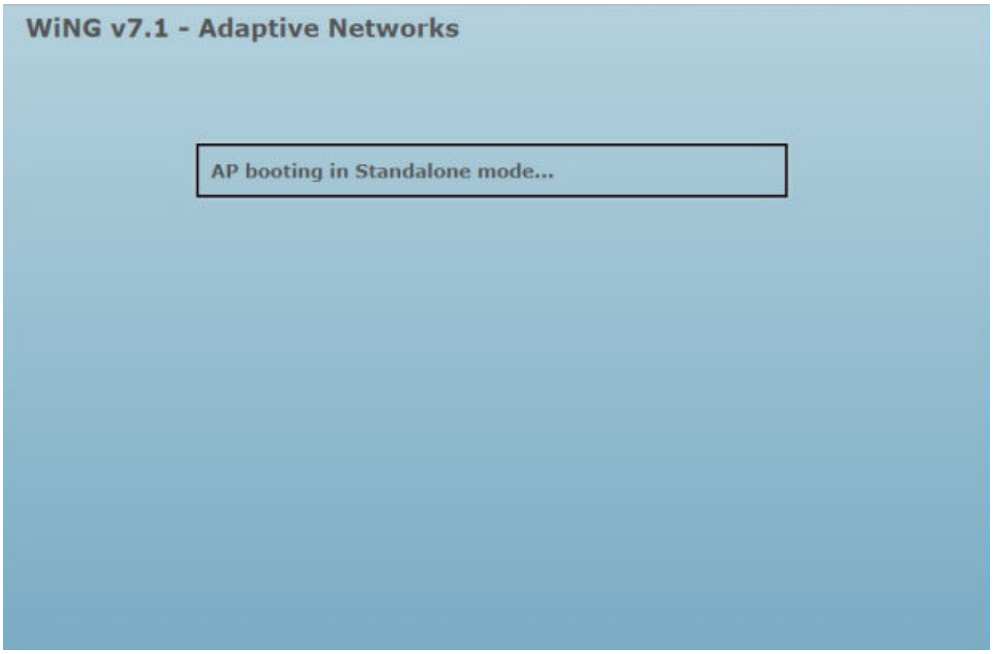
The secondary IP address will be: *169.254.**240.10***

You will be presented with the following screen:



2 Click the **Standalone** button to move into the `Standalone/WiNG` mode.

The following screen displays:



3 After the AP has rebooted, use the following default credentials to login:

username: `admin`

password: `admin123`

Resetting an AP's Mode of Operation

This section describes how to reset an adopted or standalone AP's mode of operation.

Once an AP's mode of operation is set to 'Centralized' or 'Distributed', and the AP is in the adopted state, you can reset the AP's mode of operation through the adopter.

For information on resetting the mode of operation of an AP adopted to WiNG VC/Controller or a Standalone AP, refer to Resetting Distributed AP's Mode of Operation on page 1955.

For information on AP adopted to ExtremeCloud Appliance, please refer to the ExtremeCloud Appliance User Guide available at https://extremenetworks.com/documentation.

Resetting Distributed AP's Mode of Operation

Resetting mode of operation of an AP adopted to WiNG VC or WiNG Controller

To revert an AP5XX, adopted to a WiNG VC or WiNG Controller, to factory-default mode of operation (that is, mode not specified) issue the following command on the WiNG VC/Controller:

```
#factory-reset deep <AP-HOSTNAME>
```

Note
The <AP-HOSTNAME> parameter represents the host name of the AP on which the command is to be implemented.

The AP's adoption status is lost, it reboots immediately with its mode of operation not specified.

Resetting a standalone AP's mode of operation

To reset a standalone AP to the 'Centralized' mode, on the AP, issue the following command:

```
#operational-mode centralized
#reload
```

Or

Follow the steps below to reset the AP to factory-default mode of operation (that is, mode not specified).

1 Access the AP's console.
2 Enter the following login credentials:

username	`resetDeep` (with 'D' in upper case)
password	`FactoryDefaultDeep` (with 'F', 'D' and 'D' in upper case)

Note
The AP reboots in the temporary 'Centralized' mode.

Resetting Centralized AP's Mode of Operation

This section describes how to revert the mode of operation of an AP operating in the 'Centralized' mode.

If the AP boots up in the 'Centralized' mode, use the following command to reset the mode of operation to factory-default setting (that is, not specified). Issue the command on the AP.

```
#cset factoryDefault deep
```

When you issue the above command, the AP reboots and moves into the discovery mode, where it tries to discover its mode of operation.

To reset the mode of operation to *Distributed*, issue the following command in the AP's configuration context:

```
#cset personality distributed
```

The AP to controller adoption is lost, the AP reboots and moves into adopter discovery mode.

C AP5XX REV AA Upgrade Procedure

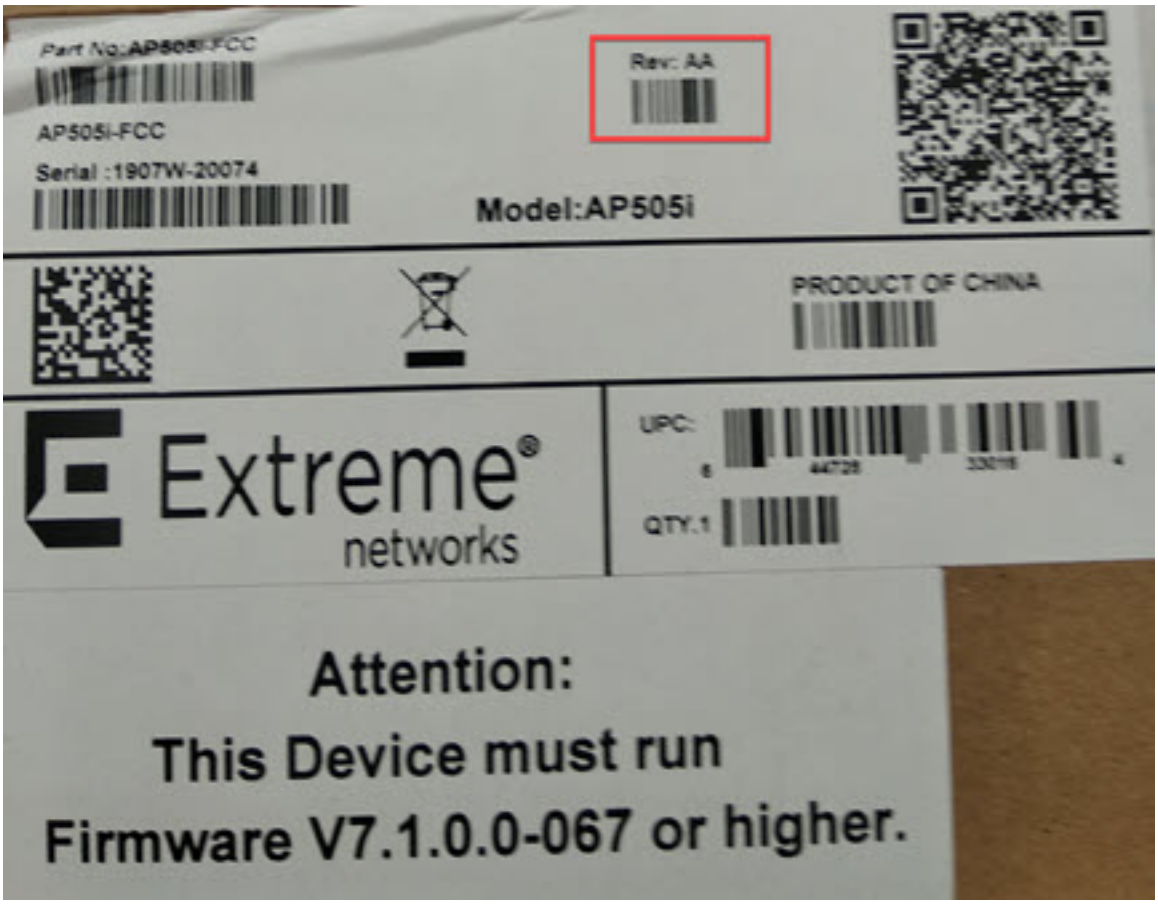
Introduction

The initial units of AP505 and AP510 model access points have been shipped with a pre-production firmware version loaded. To get these units operational, you will need to upgrade them to the official WiNG 7.1.0.0-138R firmware version.

This chapter describes the procedure to be followed to upgrade 'Rev: AA' AP505/AP510 model access points to the latest image.

How to determine if your AP requires an upgrade?

To begin with, determine if your AP505/AP510 requires a software upgrade. Check the label on the access point box for the 'Hardware Revision Version'. If the revision version reads 'Rev: AA' the access point must be upgraded.



Bulk 'Rev: AA' AP505/AP510 Upgrade through Virtual Controller

This section describes how to do a bulk upgrade of 'Rev: AA' AP505 and AP510 access points in the absence of a WiNG Controller or ExtremeCloud Appliance.

If you have multiple 'Rev: AA' AP505 and AP510 access points and no WiNG Controller or ExtremeCloud Appliance deployed in your network, configure one of the AP as a *Virtual Controller* (VC). Use this virtual controller AP to perform a bulk upgrade of the other APs.

The steps below describe how to perform this task:

1 Set the AP's 'operational-mode' to 'standalone/distributed'. You can either use the AP's CLI or GUI to set the AP's operational mode.

Note

The WiNG 7.1.X AP505 and AP510 model access points have the capability of operating in the following two modes: **`Distributed`** and **`Centralized`**. For a newly-manufactured, out-of-the-box AP505 and AP510 access point the mode of operation is *not specified*. The *Centralized* mode of operation is ideally suited for dense localized deployments, while the *Distributed* mode supports scaled-out deployments.

a Access the AP's CLI through the console or SSH.

For SSH, use the AP's Primary or Secondary IP address.

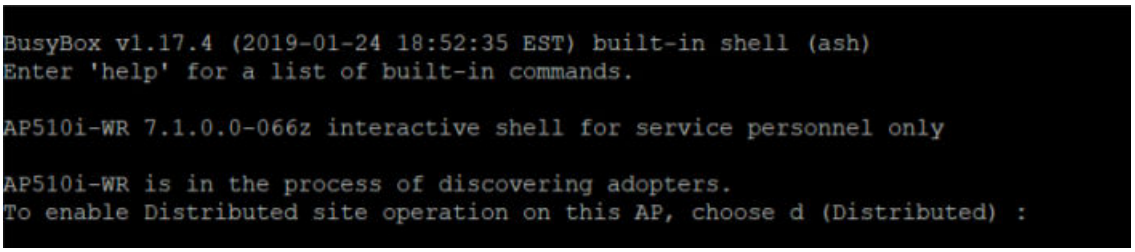
Primary IP address - This is the DHCP provided IP address.

Secondary IP address - This is the ZEROCONF IP address printed on the box.

You will be prompted to provide the login credentials. Since, this is a fresh, out-of-box device, you will have to enter the default credentials.

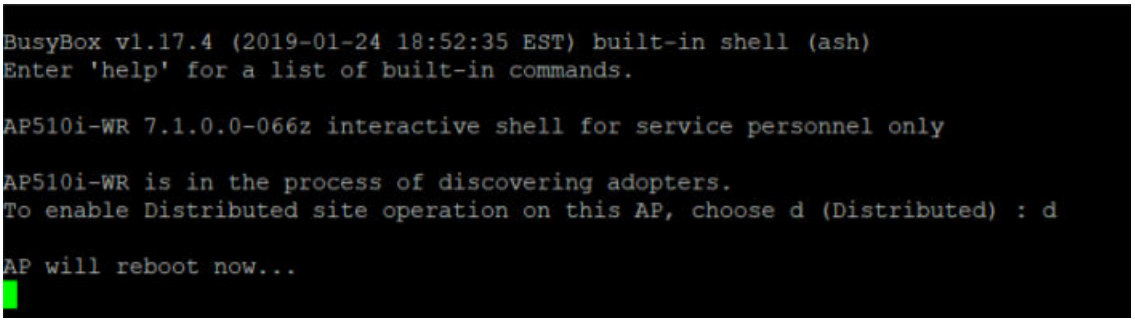
b Enter the default credentials `admin/admin123`.

You will be prompted: '**To enable distributed site operation on this AP, choose d (Distributed):**'



c Type 'd'.

The following message is displayed:



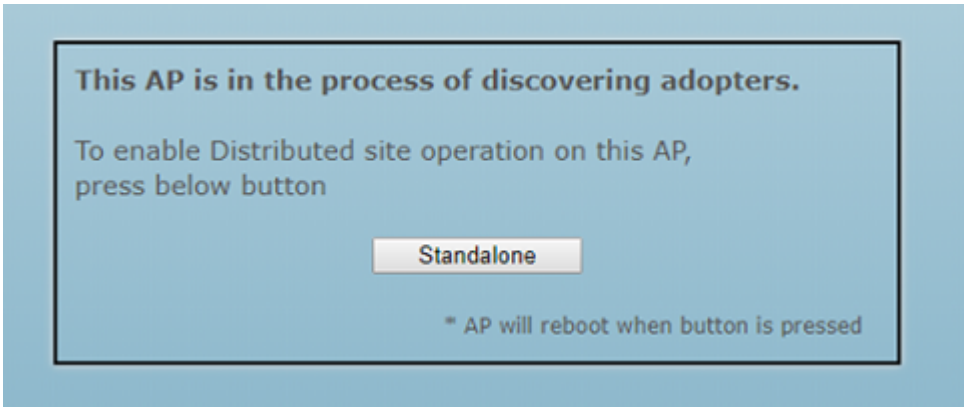
Note
The AP will reboot in the standalone/distributed operational mode.

d Alternately, access the AP's GUI by pointing the Web browser to the AP's Primary or Secondary IP address. (http://<AP-IP-ADDRESS>)

Primary IP address - This is the DHCP provided IP address.

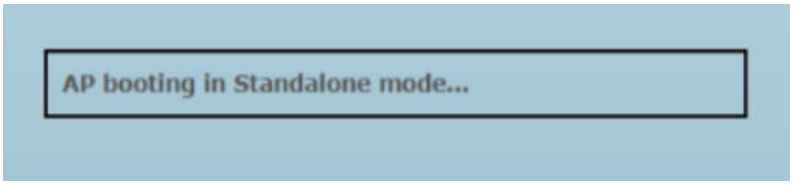
Secondary IP address - This is the ZEROCONF IP address printed on the box.

The following message is displayed:



e Click on the “Standalone” button.

The following message is displayed:



Note
The AP will reboot in the standalone/distributed operational mode.

2 After the AP's operational-mode is set to 'standalone/distributed', upgrade it to the 7.1.0.0-138R firmware version.

a Access the AP's CLI through the console or SSH.

b Enter `admin/admin123` as username/password.

The AP's CLI opens in the user executable mode.

```
ap5xx-xxxxxx>
```

c Enter 'enable' to move into the privileged mode.

```
ap5xx-xxxxxx>enable
ap5xx-xxxxxx#
```

d Use following command to upgrade AP to the latest firmware:

```
ap5xx-xxxxxx#upgrade tftp://<hostname|IP>path/filename
```

Note
Ensure that the latest 7.1.0.0-138R image file is availabe at the specified location.

e Reload the AP, after the upgrade.

```
ap5xx-xxxxxx#reload
```

3 Add the other 'Rev: AA' AP5XXs to the network, in the same VLAN as the first AP that is being configured as a VC.

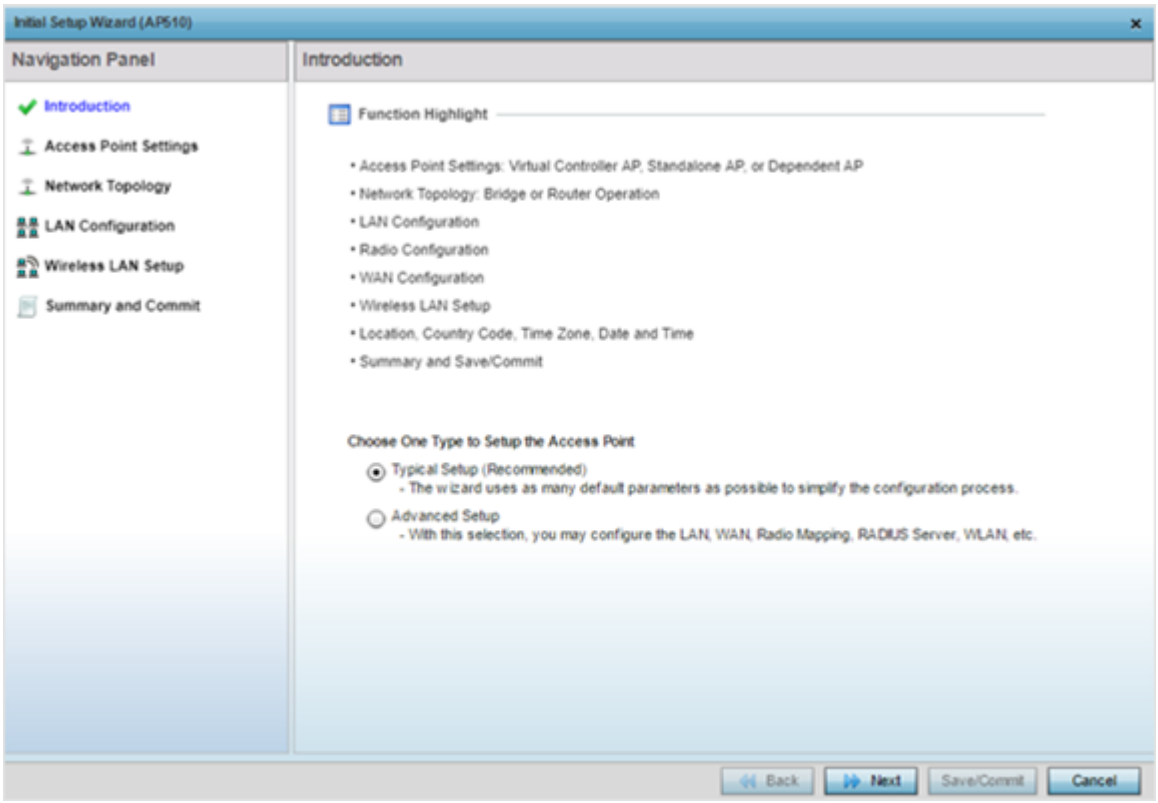
The APs will reload twice and boot up in the 'Distributed' operational mode.

4 Access the first upgraded AP's GUI, by pointing the Web browser to the AP's Primary (DHCP-provided) or Secondary (ZEROCONF) IP address.

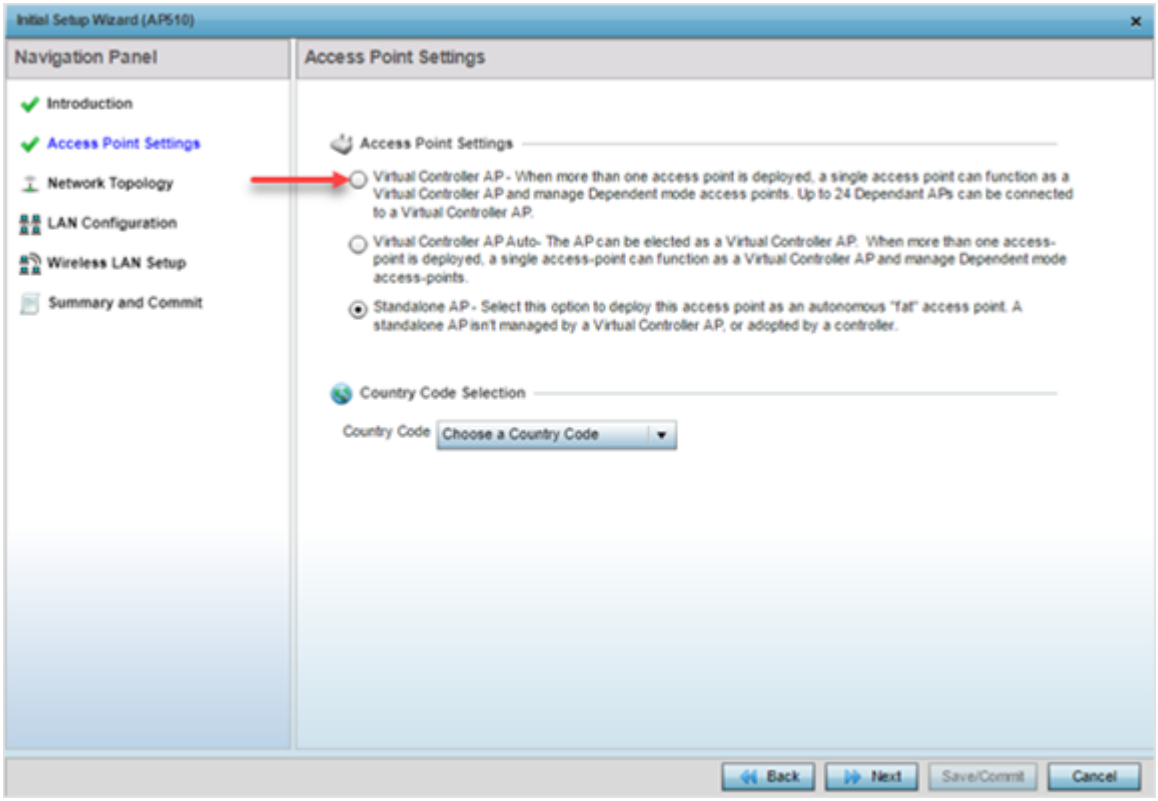
The login page is displayed.

5 Enter credentials `admin/admin123`.

6 Use the Initial Setup Wizard to configure the AP as a Virtual Controller.



7 Click **Next**.



8 On the Access Point Settings screen, select the **Virtual Controller AP** radio button.

The AP is now configured as a VC. At this point, the other 'Rev: AA' APs in the VLAN will adopt to the virtual controller AP.

9 Use the following CLI command to load the AP image file on to the VC.

```
ap5xx-xxxxxx#device-upgrade load-image ap5XX tftp://<hostname|IP>/path/file
```

Note
Once the AP image file upload is complete, the other adopted APs will be upgraded by the VC AP.

Bulk 'Rev:AA' AP5XX Upgrade through WiNG Controller/ ExtremeCloud Appliance

Consider a scenario consisting of multiple 'Rev:AA' AP505/AP510 access points and a WiNG Controller or ExtremeCloud Appliance adopting the access points. In this case, the 'Rev: AA' APs get upgraded through the adopting device.

Note
To be able to adopt and upgrade AP505/AP510 model access points, WiNG Controllers need to run version WiNG 7.1.0.0 and ExtremeCloud Appliance needs to run version 4.36.01.

Note

The WiNG 7.1.X AP505 and AP510 model access points have the capability of operating in the following two modes: **`Distributed`** and **`Centralized`**. For a newly-manufactured, out-of-the-box AP505 and AP510 access point the mode of operation is *not specified*. The *Centralized* mode of operation is ideally suited for dense localized deployments, while the *Distributed* mode supports scaled-out deployments.

1 Deploy the 'Rev: AA' AP505/AP510 access points.

The APs will boot up with the operational-mode not specified.

2 After booting up, the APs run the discovery image to determine their mode of operation.

Note

Based on the discovery methods found in the network, the operational-mode is set to either 'Distributed' or 'Centralized'.

3 The APs then try to discover and adopt to an adopter.

Note

Based on the network-provided discovery mechanism (that is, DHCP or DNS), the APs discover and adopt either to a WiNG Controller or the ExtremeCloud Appliance.

The following adoption scenarios are possible for the two modes of operation:

- AP in Distributed mode — can adopt to a WiNG VC, WiNG Controller or ExtremeCloud Appliance
- AP in Centralized mode — can adopt to ExtremeCLoud Appliance

4 In case of ExtremeCloud Appliance adoption, the APs will be automatically upgraded to the latest firmware post adoption.

5 In case of WiNG Controller adoption, the APs will be upgraded by the Controller based on device upgrade settings configured on the Controller (auto upgrade upon adoption or on demand upgrade).

Glossary

AAA

Authentication, Authorization, and Accounting is a system in IP-based networking to control which computer resources specific users can access and to keep track of the activity of specific users over the network.

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BGP

Border Gateway Protocol is a router protocol in the IP suite designed to exchange network reachability information with BGP systems in other autonomous systems. You use a fully meshed configuration with BGP.

BGP provides routing updates that include a network number, a list of ASs that the routing information passed through, and a list of other path attributes. BGP works with cost metrics to choose the best available path; it sends updated router information only when one host has detected a change, and only the affected part of the routing table is sent.

BGP communicates within one AS using Interior BGP (IBGP) because BGP does not work well with IGP. Thus the routers inside the AS maintain two routing tables: one for the IGP and one for IBGP. BGP uses exterior BGP (EBGP) between different autonomous systems.

Bonjour

Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and services that these computers offer over a local network. Bonjour provides a general method to discover services on a local area network (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners, and filesharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

captive portal

A browser-based authentication mechanism that forces unauthenticated users to a web page.

CDP

Cisco Discovery Protocol is a proprietary Data Link Layer protocol that shares information about other directly connected Cisco equipment, such as operating system versions and IP addresses.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DHCP

Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DoS

Denial-of-service. See *DoS attack*.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable

from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond

ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud Appliance

The ExtremeCloud Appliance, the newest addition to the Smart OmniEdge portfolio, is a next generation orchestration application offering all the mobility services required for modern unified access deployments. The ExtremeCloud Appliance extends the simplified workflows of the ExtremeCloud public cloud application to on-prem/private cloud deployments.

The ExtremeCloud Appliance includes comprehensive critical network services for wireless and wired connectivity, wireless device secure onboarding, distributed and centralized data paths, role-based access control through the Application Layer, integrated location services, and IoT device onboarding through a single platform.

Built on architecture with the latest technology, the embedded operating system supports application containers that enable future expansion of value added applications for the unified access edge. Learn more about ExtremeCloud Appliance at https://www.extremenetworks.com/product/extremecloud-appliance/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeControl

ExtremeControl, formerly Extreme Access Control™ (EAC), is a set of management software tools that use information gathered by a hardware engine to control policy to all devices on the network. The software allows you to automate and secure access for all devices on the network from a central dashboard, making it easier to roll out security and identity policies across the wired and wireless network. Learn more about ExtremeControl at https://www.extremenetworks.com/product/extremecontrol/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeWireless WiNG

The WiNG architecture is a solution designed for 802.11n and 802.11ac networking. It is designed for standalone or distributed hierarchical networks. The ExtremeWireless WiNG software distributes intelligence right to the network edge, empowering every controller and access point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time. It is highly scalable and well suited to meet the needs of large, geographically distributed enterprises. It is an ideal wireless networking solution for the retail, manufacturing, transportation & logistics, and hospitality verticals.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

IPsec/IPsec-ESP/IPsec-AH

Internet Protocol Security (IPSec)	Internet Protocol security.
Encapsulating Security Payload (IPsec-ESP)	The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.
Internet Protocol security Authentication Header (IPsec-AH)	AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.

IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement VPNs.

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

IPv6

Internet Protocol version 6. IPv6 is the next-generation IP protocol. The specification was completed in 1997 by IETF. IPv6 is backward- compatible with and is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited (for all intents and purposes) number of networks and systems; IPv6 is expected to slowly replace IPv4, with the two existing side by side for many years.

LACP

Link Aggregation Control Protocol is part of the IEEE 802.3ad and automatically configures multiple aggregated links between switches.

LLDP

Link Layer Discovery Protocol conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

MAC

Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one NIC to another across a shared channel.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

PPPoE

Point-to-Point Protocol over Ethernet is a network protocol for encapsulating Point-to-Point Protocol frames inside Ethernet frames. It is mainly used with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet. It is also used in plain Metro Ethernet networks.

QoS

Quality of Service is a technique that is used to manage network resources and guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SSID

The Service Set Identifier is a 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the BSS. Several BSSs can be joined together to form one logical WLAN segment, referred to as an (ESS). The SSID is used to identify the ESS.

In 802.11 networks, each AP advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named access point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID.
Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A

device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VRRP

The Virtual Router Redundancy Protocol specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the master router, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master router become unavailable. In case the master router fails, the virtual IP address is mapped to a backup router's IP address; this backup becomes the master router. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every host. VRRP is defined in RFC 2338.

Wi-Fi

Wireless Fidelity is the official term used to refer to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term was promulgated by the Wi-Fi Alliance.

WLAN

Wireless Local Area Network.

Index