Commands Reference — ACLI
Avaya Virtual Services Platform 9000

3.2
NN46250-104, 03.02
March 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Purpose of this document

The ACLI Commands Reference provides default values and proper syntax for the Avaya Command Line Interface (ACLI) commands.

Chapter 2: New in this release

The following sections detail what is new in Avaya Virtual Services Platform 9000 Commands Reference — ACLI, NN46250–104.

Features

See the following sections for information about feature changes.

4–byte autonomous system (AS) numbers

Beginning with Release 3.2, Border Gateway Protocol (BGP) supports 4–byte AS numbers. For more information, see the following commands:

- router bgp as-4-byte enable on page 142
- router bgp as-dot enable on page 142

IGMPv3

Release 3.2 provides full support for IGMPv3 RFC3376. For more information, see the following commands:

- ip igmp igmpv3-explicit-host-tracking on page 261
- show ip igmp group on page 286

IPv6

Release 3.2 adds support for IPv6 routing. For a list of supported IPv6 commands, see IPv6 routing commands on page 301 and BGP services commands on page 113.

Application Configuration mode

Beginning with Release 3.2, Application Configuration mode is introduced as a new Avaya Command Line Interface (ACLI) Configuration mode to support VSP Talk, which allows users to monitor VSP 9000 remotely through an instant messaging client.

To enter Application Configuration mode, first log in to Privileged EXEC mode (enter `enable`) and Global Configuration mode (enter `configure terminal`), then to access Application Configuration mode enter `application`. For more information on Application mode, see *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

Lossless Ethernet

Release 3.2 adds Lossless Ethernet for 10 GbE ports to guarantee the switch does not drop certain traffic types. You can configure all unicast traffic on the port to be lossless, or you can configure only tagged unicast traffic with a specific lossless–802.1p value to be lossless. If you change the lossless-802.1p value, the change affects all priority-based flow control (PFC)

configured ports. You cannot change this value for individual lossless ports. For more information, see:

- lossless-port on page 175
- qos lossless-802.1p on page 177
- show interfaces gigabitethernet error on page 443
- show interfaces gigabitethernet lossless-config on page 180
- show qos 802.1p-override on page 502
- show qos lossless-802.1p on page 180

For conceptual information on Lossless Ethernet, see *Avaya Virtual Services Platform 9000 Planning and Engineering — Network Design*, NN46250–200. For configuration information on Lossless Ethernet, see *Avaya Virtual Services Platform 9000 Configuration — Ethernet Modules*, NN46250–508.

ACLI and SNMP log consolidation

Prior to Release 3.2, the system stored the CLI log and SNMP log in two separate files on the external flash: clilog.txt and snmplog.txt. The system did not send the SNMP log and ACLI Command logs to the syslog server.

In Release 3.2, the ACLI command and SNMP logs are included in the main system log file, which can be sent to an external syslog server.

The following commands are obsolete:

- **clilog maxfilesize <64–256000>**
- **clilog syslog-host enable**
- **snmplog maxfilesize <64–256000>**

The commands **show logging file module clilog** and **show logging file module snmplog** replace previous commands to show ACLI and SNMP logs. The following commands are only applicable to log files generated by past releases prior to Release 3.2:

- **show clilog file**
- **save clilog file**
- **copy clilog WORD <1–255>**
- **show snmplog file**
- **save snmplog file**

For more information, see:

- clilog on page 547
- show clilog on page 570
- save clilog on page 567
- save snmplog on page 569

- snmplog on page 581
- show logging file on page 573

Other changes

See the following sections for information about changes that are not feature-related.

Purpose of this document

To improve documentation usability, a brief description of the purpose of this document is now the first chapter.

Chapter 3: Administration commands

This chapter describes Avaya Command Line Interface (ACLI) commands to support the administration of the Avaya Virtual Services Platform 9000.

access-policy

Configure an access policy to control access to the switch. You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service, you can also specify the level of access; for example, read-only or read/write/all. Use the command without parameters to globally enable access policies.

Syntax

```
access-policy <1-65535> access-strict

access-policy <1-65535> accesslevel { ro | rwa | rw }

access-policy <1-65535> enable

access-policy <1-65535> ftp

access-policy <1-65535> host WORD<0-46>

access-policy <1-65535> http

access-policy <1-65535> mode { allow | deny }

access-policy <1-65535> name WORD<0-15>

access-policy <1-65535> network WORD<1-46> <0-128>

access-policy <1-65535> precedence <1-128>

access-policy <1-65535> rlogin

access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c |
usm }

access-policy <1-65535> snmpv3

access-policy <1-65535> ssh

access-policy <1-65535> telnet

access-policy <1-65535> tftp

access-policy <1-65535> username WORD<0-30>
```

```
access-policy <1-65535>
access-policy
default access-policy <1-65535> access-strict
default access-policy <1-65535> accesslevel
default access-policy <1-65535> enable
default access-policy <1-65535> ftp
default access-policy <1-65535> host
default access-policy <1-65535> http
default access-policy <1-65535> mode
default access-policy <1-65535> name
default access-policy <1-65535> network
default access-policy <1-65535> precedence
default access-policy <1-65535> rlogin
default access-policy <1-65535> snmpv3
default access-policy <1-65535> ssh
default access-policy <1-65535> telnet
default access-policy <1-65535> tftp
default access-policy <1-65535> username
default access-policy <1-65535>
default access-policy
no access-policy <1-65535> access-strict
no access-policy <1-65535> enable
no access-policy <1-65535> ftp
no access-policy <1-65535> host
no access-policy <1-65535> http
no access-policy <1-65535> network
no access-policy <1-65535> rlogin
no access-policy <1-65535> snmp-group WORD<1-32> { snmpv1 | snmpv2c |
usm }
no access-policy <1-65535> snmpv3
no access-policy <1-65535> ssh
```

no access-policy <1-65535> telnet

no access-policy <1-65535> tftp

no access-policy <1-65535>

no access-policy

Parameters

Variable	Value
access-strict	Specifies the level of access if you configure the policy to allow access. The access-strict parameter ties to the accesslevel parameter. If you enable access-strict, the access policy looks at the `accesslevel` parameter, and only applies to that access level. If you disable access-strict (false), the policy looks at the value for accesslevel, and then the system applies the policy to anyone with equivalent rights or higher.
accesslevel <*ro*|*rwa*|*rw*>	Restrains access to criteria specified in the access policy. • true—the system accepts only the currently configured access level • false—the system accepts access up to the configured level
enable	Activates the access policy.
ftp	Activates or disables FTP for the specified policy. Because FTP derives its login and password from the ACLI management filters, FTP works for read-write-all (rwa) and read-write (rw) access but not for the read-only (ro) access.
host *WORD<0–46>*	For remote login access, specifies the trusted host address as an IP address.
http	Activates the HTTP for this access policy.
mode <*allow*|*deny*>	Specifies whether the designated network address is allowed access to the system

Variable	Value
	through the specified access service. The default is allow.
name *WORD<0–15>*	Specifies a name expressed as a string from 0–15 characters.
network *<A.B.C.D>* *<A.B.C.D>*	Specifies the IP address and subnet mask that can access the system through the specified access service.
precedence *<1-128>*	Specifies a precedence value for a policy, expressed as a number from 1–128. The precedence value determines which policy the system uses if multiple policies apply. Lower numbers take higher precedence.
rlogin	Activates remote logon for the access policy.
snmp-group *WORD<1–32>* *<snmpv1|snmpv2c|usm>*	Adds an snmp-v3 group under the access policy. *WORD<1–32>* is the snmp-v3 group name of 1–32 characters. *<snmpv1|snmpv2|usm>* is the security model; either snmpv1, snmpv2c, or usm.
snmpv3	Activates SNMP version 3 for the access policy.
ssh	Activates SSH for the access policy.
telnet	Activates Telnet for the access policy.
tftp	Activates the Trivial File Transfer Protocol for this access policy.
username *WORD<0–30>*	Specifies the trusted host user name for remote login access.

Default

The following list provides the default values for the applicable command parameters:

- access-strict: disabled (false)
- accesslevel: ro
- enable: disabled (off)
- ftp: disabled
- http: disabled
- mode: allow
- name: none

- precedence: 10
- rlogin: disabled
- snmpv3: disabled
- ssh: disabled
- telnet: disabled
- tftp: disabled
- username: none

Command mode

Global Configuration mode

access-policy by-mac

Configure access-policies by MAC address to allow or deny local MAC addresses on the network management port after an access policy is activated. If the source MAC does not match a configured entry, then the default action is taken.

Syntax

access-policy by-mac action { allow | deny }

access-policy by-mac 0x00:0x00:0x00:0x00:0x00:0x00 { allow | deny }

default access-policy by-mac action

default access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>

no access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00>

Parameters

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00> <allow|deny>	Adds a MAC address to the policy. Enter the MAC address in hexadecimal format. Specify the action to take for the MAC address.
action *<allow|deny>*	Specifies the action for a MAC address that does not match the policy.

Default

The default action is allow.

Command mode

Global Configuration mode

application

Log on to Application mode.

Syntax

`application`

Parameters

None

Default

None

Command mode

Global Configuration mode

auto-negotiate (for the management port)

Configure auto-negotiation for the Ethernet management port.

Syntax

`auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`

`default auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`

`no auto-negotiate [port {slot/port[-slot/port][,...]}] [enable]`

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port.

Default

The default is enabled.

Command mode

mgmtEthernet Interface Configuration mode

auto-recover-delay

Set the time delay for the automatic recovery of ports.

Syntax

auto-recover-delay <5–3600>

default auto-recover-delay <5–3600>

no auto-recover-delay <5–3600>

Parameters

Variable	Value
<5–3600>	Specifies the range to be set for the auto-recovery of ports in seconds. The range varies between 5 to 3600 seconds.

Default

The default is 30.

Command mode

Global Configuration mode

autotopology

Configure the SynOptics Network Management Protocol (SONMP) to allow a network management station (NMS) formulate a map that shows the interconnections between Layer 2 devices in a network.

Syntax

autotopology

default autotopology

no autotopology

Parameters

None.

Default

The default status is enabled.

Command mode

Global Configuration mode

banner

Configure the ACLI logon banner to display a warning message to users before authentication.

Syntax

banner custom

banner static

banner WORD<1–80>

banner motd WORD<1–1516>

banner displaymotd

default banner

default banner motd

default banner displaymotd

no banner

no banner motd

no banner displaymotd

Parameters

Variable	Value
custom	Activates the custom banner.
displaymotd	Activates or disables the message of the day.
motd *WORD<1–1516>*	Creates a message of the day to display with the logon banner. To provide a string with spaces, include the text in quotation marks (").
static	Activates static banner.
WORD<1–80>	Adds lines of text to the ACLI logon banner.

Default

The default configuration uses the default banner with no message of the day.

Command mode

Global Configuration mode

boot

Restart the switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify an optional configuration file to use to load the device. If no config file is specified, the run-time ACLI uses the configuration file specified by the boot config choice command. The image booted is that specified by the software activate command.

Syntax

boot [config WORD<1–99>] [-y]

Parameters

Variable	Value
config *WORD<1–99>*	Specifies the software configuration device and file name in one of the following formats: • /intflash/<file> • /extflash/<file> • /usb/<file> The file name, including the directory structure, can include up to 99 characters
-y	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the switch restarts.

Default

None

Command mode

Privileged EXEC mode

boot config choice

Change the boot source order to change the order in which the system accesses the configuration files.

Syntax

boot config choice primary {backup-config-file|config-file} WORD<0–255>

default boot config choice primary [backup-config-file|config-file]

Parameters

Variable	Value
{backup-config-file |config-file}	Specifies that the boot source uses either the configuration file or a backup configuration file.
WORD<0–255>	Identifies the configuration file. *WORD<0–255>* is the device and file name, up to 255 characters including the path, in one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /extflash/<file> • /usb/<file>

Default

By default, the primary source is the internal flash. If you change the primary source, the system uses your configuration first, and then accesses the default locations. If the default locations do not contain a configuration or backup configuration file, the system loads the default configuration.

Command mode

Global Configuration mode

boot config delay

Configure the standby-to-master delay to set the number of seconds a standby CPU waits before trying to become the master CPU. The time delay you configure applies during a cold start; it does not apply to a failover start.

Syntax

boot config delay <0–255>

default boot config delay

Parameters

Variable	Value
<0–255>	Specifies the number of seconds a standby CPU waits before trying to become the master CPU.

Default

The default value is 10.

Command mode

Global Configuration mode

boot config flags

Configure the system flags to enable specific services and functions for the chassis.

Syntax

boot config flags block-snmp

boot config flags debug-config console

boot config flags debug-config file

boot config flags debug-config

boot config flags debugmode

boot config flags fabric-profile <1-3>

boot config flags factorydefaults

boot config flags ftpd

boot config flags ha-cpu

boot config flags hsecure

boot config flags logging

boot config flags reboot

boot config flags rlogind

boot config flags savetostandby

boot config flags spanning-tree-mode mstp

boot config flags spanning-tree-mode rstp

boot config flags sshd

```
boot config flags telnetd
boot config flags tftpd
boot config flags trace-logging
boot config flags verify-config
boot config flags wdt
default boot config flags block-snmp
default boot config flags debug-config
default boot config flags debugmode
default boot config flags fabric-profile
default boot config flags ftpd
default boot config flags ha-cpu
default boot config flags hsecure
default boot config flags logging
default boot config flags reboot
default boot config flags rlogind
default boot config flags savetostandby
default boot config flags spanning-tree-mode
default boot config flags sshd
default boot config flags telnetd
default boot config flags tftpd
default boot config flags trace-logging
default boot config flags verify-config
default boot config flags wdt
no boot config flags block-snmp
no boot config flags debug-config
no boot config flags debugmode
no boot config flags factorydefaults
no boot config flags ftpd
no boot config flags ha-cpu
no boot config flags hsecure
no boot config flags logging
```

no boot config flags reboot

no boot config flags rlogind

no boot config flags savetostandby

no boot config flags spanning-tree-mode

no boot config flags sshd

no boot config flags telnetd

no boot config flags tftpd

no boot config flags trace-logging

no boot config flags verify-config

no boot config flags wdt

Parameters

Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management.
debug-config [console|file]	Activates or disables run-time debugging of the configuration file. If you activate debugging, line-by-line configuration file processing appears on the console during CPU utilization. If you change the debug-config variable value, you must restart the switch.
debugmode	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. If you enable this flag, the switch does not restart following a fatal error. If you change this parameter, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
fabric-profile <1–3>	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are • 1: balanced • 2: unicast optimized • 3: multicast optimized

Variable	Value
factorydefaults	Specifies whether the switch uses the factory default settings at startup. This flag automatically resets to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
ftpd	Activates or disables the FTP server on the switch. To enable FTP, ensure that the tftpd flag is disabled.
ha-cpu	Activates or disables High Availability (HA) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable High Availability mode, the secondary CPU resets to load settings from the saved configuration file. You must reset the master CPU after the secondary CPU starting is complete. **Caution:** **Risk of service loss** Enabling HA mode can disable certain features.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • aging time • failed login attempt limitation • designated IP address filtration If you enable High Secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.
logging	If an external flash device exists in the system, you can use the logging command to activate or disable system logging to a file on the external flash. The system names log files according to the following: • File names appear in 8.3 (xxxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address.

Variable	Value
	• The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file. The system generates multiple sequence numbers for the same chassis and same slot if • you replace the CPU • you reinsert the CPU • the system reaches the maximum log file size
reboot	Activates or disables automatic reboot on a fatal error. The reboot command is equivalent to the debugmode command. If you change the reboot variable value, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.
rlogind	Activates or disables the rlogin and rsh server.
savetostandby	Activates or disables automatic save of the configuration file to the standby CPU. If you operate a dual CPU system, Avaya recommends that you enable this flag for ease of operation.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. If you change the spanning tree mode, you must save the current configuration and restart the switch.
sshd	Activates or disables the SSH server service.
telnetd	Activates or disables the Telnet server service. If you disable the Telnet server service in a dual CPU system, the Telnet server prevents a Telnet connection initiated from the other CPU.
tftpd	Activates or disables Trivial File Transfer Protocol server service. If you disable the

Variable	Value
	TFTP server you can still copy files between the CPUs.
trace-logging	Activates or disables the creation of trace logs. **Important:** Do not change this parameter unless directed by Avaya.
verify-config	Activates syntax checking of the configuration file. If the system finds a syntax error, it loads the factory default configuration. If you disable this flag, the system logs syntax errors and the CPU continues to source the configuration file. Avaya recommends that you disable the verify-config flag. If you change this parameter, you must restart the switch.
wdt	Activates or disables the hardware watchdog timer monitoring a hardware circuit. The watchdog timer restarts the switch based on software errors. If you change the wtd flag, you must restart the switch. **Important:** Do not change this parameter unless directed by Avaya.

Default

The following list provides the default values for the applicable command parameters:

- block-snmp: disabled
- debug-config: console
- debugmode: disabled
- fabric-profile: 1, balanced
- factorydefaults: disabled
- ftpd: disabled
- ha-cpu: disabled
- hsecure: disabled
- logging: enabled
- reboot: enabled
- rlogind: disabled
- savetostandby: disabled

- spanning-tree-mode: MSTP
- sshd: disabled
- telnetd: disabled
- tftpd: disabled
- trace-logging: disabled
- verify-config: enabled
- wdt: enabled

Command mode

Global Configuration mode

boot config loadconfigtime

Set the timeout for loading the configuration file.

Syntax

boot config loadconfigtime <0–300>

default boot config loadconfigtime <0–300>

Parameters

Variable	Value
<0–300>	Specifies the timeout for loading the configuration file in seconds.

Default

None

Command mode

Global Configuration mode

boot config sio console

Configure the serial port devices to define connection settings for the console port .

Syntax

boot config sio console 8databits

boot config sio console baud <9600–115200>

default boot config sio console 8databits

default boot config sio console baud

no boot config sio console 8databits

Parameters

Variable	Value
8databits	Specifies either 8 (activated) or 7 (disabled) data bits for each byte for the software to interpret.
<9600–115200>	Configures the baud rate for the port.

Default

The default databits is 8. The default baud rate is 9600.

Command mode

Global Configuration mode

cli timeout

Configure the idle timeout period before automatic logoff for ACLI and Telnet sessions.

Syntax

cli timeout <30-65535>

default cli timeout

Parameters

Variable	Value
<30-65535>	Configures the timeout value, in seconds, to wait for a Telnet or ACLI login session before terminating the connection.

Default

The default is 900 seconds.

Command mode

Global Configuration mode

Configure network

Syntax

`configure network address {A.B.C.D} [filename WORD<1–239>]`

`configure terminal`

Parameters

Variable	Value
address *{A.B.C.D}*	Specify an address of the TFTP server.
filename *WORD<1–239>*	Specify the filename of the configuration file.
network	Configures the device from a TFTP network host.
terminal	Logs on to Global Configuration mode.

Default

Command mode

Privileged EXEC mode

cp

Use this command to copy files.

Syntax

`cp WORD<1-255> WORD<1-255> -y`

`cp WORD<1-255> WORD<1-255>`

Parameters

Variable	Value
WORD <1–255> WORD <1–255>	The first *WORD<1–255>*specifies the file to copy. The second *WORD<1–255>* uses one of the following formats: • /intflash/ <file> • /extflash/ <file>

Variable	Value
	• /usb/<file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> /mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP will support /mnt/intflash and /mnt/extflash in this release. *Word<1–255>* is a string of 1–255 characters.
-y	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action.

Default

None

Command mode

Privileged EXEC mode

cp-limit

Configure the CP Limit functionality to protect the switch from becoming congested by an excess of data flowing through one or more ports.

Syntax

cp-limit <1000–20000> [shutdown]

cp-limit [port {slot/port[-slot/port][,...]}] [<1000–20000>] [shutdown]

default cp-limit [port {slot/port[-slot/port][,...]}]

no cp-limit [port {slot/port[-slot/port][,...]}] [shutdown]

Parameters

Variable	Value
<1000–20000>	Specifies the packet rate value in the range of 1000 to 20000. The value determines the

Variable	Value
	number of packets coming to the CP every second.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2). **Note:** Port option is not available if cp-limit is configured using MLT Interface Configuration mode.
shutdown	Enables the shutdown of the port.

Default

The default limit is 5000.

Command mode

GigabitEthernet Interface Configuration mode or MLT Interface Configuration mode

delete

Use this command to delete files.

Syntax

`delete WORD<1-255> -y`

`delete WORD<1-255>`

Parameters

Variable	Value
WORD<1–255>	Specifies the name and location of the file to delete in one of the following formats: • /intflash/ <file> • /extflash/ <file> • /usb/<file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> /mnt/intflash is equivalent to the /intflash of the standby CP (if present).

Variable	Value
	/mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP will support /mnt/intflash and /mnt/extflash in this release. *WORD<1–255>* is a string of 1–255 characters.
-y	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch deletes the file.

Default

None

Command mode

Privileged EXEC mode

duplex (for the management port)

Configure the duplex mode for the Ethernet management port.

Syntax

`duplex [port {slot/port[-slot/port][,...]}]<half|full>`

`default duplex [port {slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
`<half|full>`	Specifies half- or full-duplex mode.
`port {slot/port[-slot/port][,...]}`	Identifies the slot and port the following format: a single slot and port (2/1).

Default

The default is half-duplex mode.

Command mode

mgmtEthernet Interface Configuration mode

enable

Use this command to enter Privileged EXEC mode in ACLI.

Syntax

`enable`

Parameters

None

Default

None

Command mode

All modes

end

Use this command to return to the Privileged EXEC mode.

Syntax

`end`

Parameters

None

Default

None

Command mode

All command modes

exit

Use this command to exit a command mode and enter the lower command mode.

Syntax

`exit`

Parameters

None

Default

None

Command mode

All modes

help

Use this command to see parameters for a particular command.

Help may be requested at any point by entering a question mark after a command, which shows the available options.

Syntax

help [WORD<1–255>]

Parameters

Variable	Value
WORD<1–255>	Enter a command to see the options for that command.

Default

None

Command mode

Privilege EXEC mode

ip domain-name

Configure the Domain Name Service (DNS) to establish the mapping between a name and an IP address.

Syntax

ip domain-name WORD<0–255>

default ip domain-name

no ip domain-name

Parameters

Variable	Value
WORD<0–255>	Configures the default domain name.

Default

None

Command mode

Global Configuration mode

ip name-server

Add addresses for DNS servers.

Syntax

ip name-server <primary|secondary|tertiary> WORD<0–46>

default ip name-server <primary|secondary|tertiary>

no ip name-server <primary|secondary|tertiary>

Parameters

Variable	Value
<primary|secondary|tertiary>*WORD<0–46>*	Configures the primary, secondary, or tertiary DNS server address. Enter the IP address in a.b.c.d format for IPv4 (string length 0–46). You can specify the IP address for only one server at a time; you cannot specify all three servers in one command.

Default

None

Command mode

Global Configuration mode

ipv6 interface address (for the management port)

Configure the IPv6 address for the Ethernet management port.

Syntax

ipv6 interface address WORD<0–255>

no ipv6 interface address WORD<0–255>

Parameters

Variable	Value
WORD<0–255>	Assigns an IPv6 address to the management port.

Default

None.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface enable (for the management port)

Enable IPv6 route advertisement on the Ethernet management port.

Syntax

ipv6 interface enable

no ipv6 interface enable

default ipv6 interface enable

Parameters

None

Default

The default is disabled.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface hop-limit (for the management port)

Configures the maximum number of hops before packets drop.

Syntax

`ipv6 interface hop-limit <1–255>`

`default ipv6 interface hop-limit`

Parameters

Variable	Value
<1–255>	Configures the maximum hops.

Default

The default is 30 hops.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface link-local (for the management port)

Creates a link-local address for the Ethernet management port.

Syntax

`ipv6 interface link–local WORD<0–19>`

Parameters

Variable	Value
WORD<0–19>	Specifies the link-local address for the management port.

Default

None

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface mtu (for the management port)

Configure the maximum transmission unit for the Ethernet management port.

Syntax

`ipv6 interface mtu <1280–9500>`

default ipv6 interface mtu

Parameters

Variable	Value
<1280–9500>	Configures the maximum transmission unit for the interface: 1280–1500, 1850, or 9500.

Default

The default is 1500.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface name (for the management port)

Configures an interface description for the Ethernet management port.

Syntax

ipv6 interface name WORD<0–255>

Parameters

Variable	Value
WORD<0–255>	Assigns a descriptive name to the management port.

Default

None.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface reachable-time (for the management port)

Configures the time a neighbor is considered reachable after receiving a reachability confirmation.

Syntax

ipv6 interface reachable-time <1–3600000>

`default ipv6 interface reachable-time`

Parameters

Variable	Value
<1–3600000>	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

Default

The default is 30000.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 interface retransmit-timer (for the management port)

Configures the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Syntax

`ipv6 interface retransmit-timer<1-4294967295>`

`default ipv6 interface retransmit-timer`

Parameters

Variable	Value
<1-4294967295>	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Default

The default is 1000.

Command mode

mgmtEthernet Interface Configuration mode

ipv6 nd dad-ns (for the management port)

Configures the number of neighbor solicitation messages from duplicate address detection.

Syntax

ipv6 nd dad-ns <0–600>

default ipv6 nd dad-ns

Parameters

Variable	Value
<0–600>	Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions

Default

The default is 1.

Command mode

mgmtEthernet Interface Configuration mode

link-flap-detect

Configure link flap detection to control link state changes on a physical port.

Syntax

link-flap-detect <auto-port-down|frequency <1–9999>|interval <2–600>|send-trap>

default link-flap-detect <auto-port-down|frequency|interval|send-trap>

no link-flap-detect <auto-port-down|send-trap>

Parameters

Variable	Value
auto-port-down	Activates automatic disabling of the port if the link-flap threshold is exceeded.
frequency <*1–9999*>	Configures the number of changes that are allowed during the time specified by the **`interval`** command.
interval <*2–600*>	Configures the link-flap-detect interval in seconds.
send-trap	Activates sending traps.

Default

The following list provides the default values for the command parameters:

- auto-port-down: disabled
- frequency: 20
- interval: 60
- send-trap: enabled

Command mode

Global Configuration mode

load-license

Load a license file to unlock the licensed features.

Syntax

`load-license`

Parameters

None

Default

None

Command mode

Global Configuration mode

login-message

Change the login prompt for ACLI.

Syntax

login-message WORD<1-1513>

default login-message

no login-message

Parameters

Variable	Value
WORD<1-1513>	Changes the ACLI logon prompt. *WORD<1-1513>* is an (American Standard Code for Information Interchange) (ASCII) string from 1–1513 characters.

Default

The default is Login.

Command mode

Global Configuration mode

loop-detect

Configure loop detect to determine if the same MAC address appears on different ports. Use the ARP-Detect feature to account for ARP packets on IP configured interfaces.

Syntax

loop-detect [action <mac-discard|port-down>] [arp-detect]

default loop-detect

no loop-detect

Parameters

Variable	Value
action <mac-discard|port-down>	Specifies the loop detect action to be taken:

Variable	Value
	• mac-discard. ARP-Detect does not support this action. • port-down shuts down the port if the system detects a flapping MAC address
arp-detect	Activates ARP-Detect.

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration mode

mac-flap-time-limit

Configure the interval at which MAC addresses are monitored by loop detection.

Syntax

`mac-flap-time-limit <10–5000>`

`default mac-flap-time-limit`

Parameters

None

Default

The default value is 500 milliseconds.

Command mode

Global Configuration mode

max-logins

Configure the number of supported rlogin sessions.

Syntax

`max-logins <0–8>`

`default max-logins`

Parameters

Variable	Value
<0–8>	Configures the maximum number of inbound remote ACLI logon sessions.

Default

The default is 8.

Command mode

Global Configuration mode

md5

Calculate the MD5 digest to verify the MD5 checksum. The md5 command calculates the MD5 digest for files on the internal or external flash and either displays the output on screen or stores the output in a file that you specify.

Syntax

`md5 WORD<1-99> -a`

`md5 WORD<1-99> -c`

`md5 WORD<1-99> -f WORD<1-99>`

`md5 WORD<1-99> -r`

`md5 WORD<1-99>`

Parameters

Variable	Value
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by *WORD<1–99>* with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f

Variable	Value
	option. If the checksum filename is not specified, the file /intflash/checksum.md5 is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: `Error: Checksum file <filename> not present` The -c option also • calculates the checksum of files specified by *WORD<1–99>* • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison

-f *WORD<1–99>*	Stores the result of MD5 checksum to a file on internal or external flash. If the output file specified with the
	-f
	option is one of the reserved filenames on the switch, the command fails with the error message:
	`Error: Invalid operation.`
	If the output file specified with the
	-f
	option is one of the files for which MD5 checksum is to be computed, the command fails with the error message:
	`VSP-9012:1# md5 *.cfg -f config.cfg`
	`Error: Invalid operation on file <filename>.`
	If the checksum filename specified by the -f option exists on the switch (and is not one of the reserved filenames), the following message appears on the switch:
	`File exists. Do you wish to overwrite? (y/n)`

-r	Reverses the output. Use with the -f option to store the output to a file. You cannot use the -r

Variable	Value
	option with the -c option.

Default

None

Command mode

Privileged EXEC mode

ntp

Enable Network Time Protocol (NTP) globally and create an authentication key.

Syntax

ntp [authentication-key <1-2147483647> WORD<0–8>]

ntp [interval <10-1440>]

default ntp [authentication-key <1-2147483647>]

default ntp [interval]

no ntp [authentication-key <1-2147483647>]

Parameters

Variable	Value
authentication-key*<1-2147483647> WORD<0–8>*	Creates an authentication key for MD5 authentication. *WORD<0–8>* specifies the secret key.
interval *<10-1440>*	Specifies the time interval, in minutes, between successive NTP updates. The default value is 15. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

Default

The default configuration removes the secret key. The default interval is 15 minutes.

Command mode

Global Configuration mode

ntp server

Add an IP address for an NTP server or modify existing NTP server parameters. You can configure a maximum of 10 time servers.

Syntax

ntp server {A.B.C.D} [auth-enable] [authentication-key <0-2147483647>]

ntp server {A.B.C.D} [enable]

default ntp server {A.B.C.D} [auth-enable] [authentication-key]

default ntp server {A.B.C.D} [enable]

no ntp server {A.B.C.D} [auth-enable]

no ntp server {A.B.C.D} [enable]

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address of the NTP server to add or modify.
auth-enable	Activates MD5 authentication on this NTP server.
authentication-key <*0-2147483647*>	Specifies the key ID value used to generate the MD5 digest for the NTP server. The value range is an integer from 0–2147483647.
enable	Activates the NTP server.

Default

The default configuration does not use MD5 authentication. The default authentication key is 0, which indicates disabled authentication.

Command mode

Global Configuration mode

password access-level

Enable ACLI access levels to control the configuration actions of various users

Syntax

password access-level WORD<2–8> [aging-time day <1-365>] [default-lockout-time <60-65000>] [min-passwd-len <10-20>] [password-history <3-32>]

default password access-level

default password [aging-time] [default-lockout-time] [min-passwd-len] [password-history]

no password access-level WORD<2–8>

Parameters

Variable	Value
`aging-time day <1-365>`	Configures the expiration period for passwords in days, from 1–365.
`default-lockout-time <60-65000>`	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60–65000 range.
`min-passwd-len <10-20>`	Configures the minimum length for passwords in high-secure mode.
`password-history <3-32>`	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history.
`WORD<2–8>`	Permits or blocks this access level. The available access levels are: • l1 • l2 • l3 • ro • rw • rwa

Default

By default, all access levels are permitted.

Command mode

Global Configuration mode

passwordprompt

Change the password prompt for ACLI sessions.

Syntax

passwordprompt WORD<1-1510>

default passwordprompt

no passwordprompt

Parameters

Variable	Value
WORD <1-1510>	Changes the ACLI password prompt. *WORD <1-1510>* is an ASCII string from 1–1510 characters.

Default

The default is Password.

Command mode

Global Configuration mode

peer

Access the standby CPU to make changes to the standby CPU without reconnecting to the console port on that module.

Syntax

peer {telnet|rlogin}

Parameters

Variable	Value
(telnet|rlogin)	Specifies the access method to use to connect to the standby CPU.

Default

None

Command mode

Privileged EXEC mode

prompt

Change the root level prompt or the system name for run-time mode.

Syntax

`prompt WORD <0–255>`

Parameters

Variable	Value
WORD <0–255>	Specifies the box level or root level prompt in the range of 0 to 255.

Default

None

Command mode

Global Configuration mode

rename

Use this command to rename a file.

Syntax

`rename WORD<1-255> <file>`

Parameters

Variable	Value
WORD<1-255>	*WORD<1-255>* specifies the file to rename.
WORD<1-255><file>	Specifies the file name to rename in one of the following formats: • /intflash/ <file> • /extflash/ <file> • /usb/<file>

Variable	Value
	• /mnt/intflash/ <file> • /mnt/extflash/ <file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *Word<1–255>* is a string of 1–255 characters.

Default

None

Command mode

Privileged EXEC mode

reset

Reset the platform to reload system parameters from the most recently saved configuration file.

Syntax

`reset [-y]`

Parameters

Variable	Value
`-y`	Suppresses the confirmation message before the switch resets. If you omit this parameter, you must confirm the action before the switch resets.

Default

None

Command mode

Privileged EXEC mode

restore

Use this command to restore the internal flash or the external flash from the USB device.

Important:

You must disable logging to the compact flash you want to restore before you can use the **restore** command.

Syntax

restore <intflash|extflash>

Parameters

Variable	Value
intflash	Specifies the internal flash to be restored.
extflash	Specifies the external flash to be restored.

Default

None

Command mode

Privileged EXEC mode

show access-policy

Show access policy configurations.

Syntax

show access-policy [by-mac] [snmp-group] [WORD<0–15>]

Parameters

Variable	Value
WORD<0–15>	Specifies an access policy name.
by-mac	Shows access policy by mac information.
snmp-group	Shows SNMP group information.

Default

None

Command mode

Privileged EXEC mode

show application vsptalk

Display global VSP Talk information.

Syntax

show application vsptalk

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show application vsptalk client

Display VSP Talk client information.

Syntax

show application vsptalk client

show application vsptalk client <gtalk|avaya>

Parameters

Variable	Value
client	Show VSP Talk client information.
client *<gtalk|avaya>*	Show client information for IM Group: • gtalk — Google Talk • avaya — Avaya IM

Default

None

Command mode

Privileged EXEC mode

show application vsptalk server

Dsiplay VSP Talk server information.

Syntax

show application vsptalk server

show application vsptalk server <gtalk|avaya>

Parameters

Variable	Value
server	Show VSP Talk server information.
server <*gtalk*|*avaya*>	Show server information for IM Group: • gtalk — Google Talk • avaya — Avaya IM

None

Default

None

Command mode

Privileged EXEC mode

show autotopology

View topology message status to view the interconnections between Layer 2 devices in a network.

Syntax

show autotopology nmm-table

Parameters

None

Default

None

Command mode

User EXEC mode

show basic config

Display the basic switch configuration.

Syntax

`show basic config`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show banner

Display the banner information.

Syntax

`show banner`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show boot config

Display the configuration to view current or changed settings for the boot parameters.

Syntax

show boot config <choice|flags|general|host|master|running-config [verbose]|sio>

Parameters

Variable	Value
choice	Shows the current boot configuration choices.
flags	Shows the current flag settings.
general	Shows system information.
host	Shows the current host configuration.
master	Identifies the current CP module slot configured as master and shows the current master configuration.
running-config [verbose]	Displays the current boot configuration. verbose includes all possible information. If you omit verbose, the system displays only the values that you changed from their default value.
sio	Specifies the current configuration of the CP module serial port.

Default

None

Command mode

Global Configuration mode

show brouter

Show brouter port information.

Syntax

show brouter [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies a VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show cli info

Display information about the ACLI configuration.

Syntax

`show cli info`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show cli password

Display the access, logon name, and password combinations.

Syntax

`show cli password`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show clock

Show clock configurations.

Syntax

`show clock [detail] [time-zone]`

Parameters

Variable	Value
detail	Shows detailed date information.
time-zone	Shows the local time-zone configuration.

Default

None

Command mode

Privileged EXEC mode

show fdb-filter

Show forwarding database filter information.

Syntax

`show fdb-filter`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ftp-access

Show the maximum FTP sessions.

Syntax

`show ftp-access`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ha-state

Show the state of High Availability (HA) on the system.

Syntax

`show ha-state`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show history

Show the history of all commands.

Syntax

`show history`

Parameters

None.

Default

None

Command mode

Privileged EXEC mode

show hosts

Query the DNS host for information about host addresses. You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address.

Syntax

`show hosts WORD<0-256>`

Parameters

Variable	Value
WORD<0–256>	Specifies one of the following • the name of the host DNS server as a string of 0–256 characters. • the IP address of the host DNS server in a.b.c.d format. • the IPv6 address of the host DNS server in hexadecimal format (string length 0–46).

Default

None

Command mode

Privileged EXEC mode

show ip dns

View the DNS client system status.

Syntax

show ip dns

Parameters

None

Default

None

Command mode

Global Configuration mode

show license

Display the existing software licenses on the platform.

Syntax

show license

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show link-flap-detect

Show link-flap-detect configuration.

Syntax

show link-flap-detect

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show mirror-by-port

Show mirror-by-port diagnostic information.

Syntax

show mirror-by-port WORD<1–1024> MirrorId List {1–479}

Parameters

Variable	Value
WORD<*1–1024*>	Displays mirror-by-port diagnostic information.
MirrorID List *{1–479}*	Displays the requested mirrors.

Default

None

Command mode

Privileged EXEC mode

show ntp

View the NTP server status statistics.

Syntax

show ntp [key]

show ntp [server]

show ntp [statistics]

Parameters

Variable	Value
key	Specifies to show NTP authentication key information.
server	Specifies to show NTP server information.
statistics	Specifies to show NTP statistics information.

Default

None

Command mode

Privileged EXEC mode

show running-config

Displays the current switch configuration information.

Syntax

show running-config [module <cli|sys|web|rmon|vlan|port|qos|mlt|stg|ip|diag|radius|ntp|lacp|naap|cluster|boot|filter|ipv6|slpp|nsna|vsptalk>][verbose]

Parameters

Variable	Value
module <cli|sys|web|rmon|vlan|port|qos|mlt|stg|ip|diag|radius|ntp|lacp|naap|cluster|boot|filter|ipv6|slpp|nsna|vsptalk>	Specifies the command group for which you request configuration settings.
verbose	Specifies complete list of configuration information on the switch.

Default

None

Command mode

Privileged EXEC mode

show slot

Show slot configuration for the interface modules.

Syntax

show slot <3–12>

Parameters

Variable	Value
<3–12>	Specifies the interface slot number.

Default

None

Command mode

Privileged EXEC mode

show slpp

Use Simple Loop Prevention Protocol (SLPP) information to view loop information.

Syntax

`show slpp`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show slpp interface

Show SLPP information for a port so that you can view the loop information for a port.

Syntax

`show slpp interface gigabitethernet [ {slot/port[-slot /port][,...]}]`

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots

Variable	Value
	and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show ssh

Verify that SSH services are enabled on the Virtual Services Platform 9000 and display SSH configuration information to ensure that the SSH parameters are properly configured.

Syntax

`show ssh`

Parameters

Variable	Value
`global`	Displays global system SSH information.
`session`	Displays the current session SSH information.

Default

None

Command mode

Privileged EXEC mode

show sys

Displays system status and technical information about the hardware components and software configuration.

Syntax

`show sys <action|dns|ecn-compatibility|force-msg|mgid-usage|msg-control|mtu|power|setting|software|stats|topology-ip>`

Parameters

Variable	Value
action	Shows the configuration for the system action parameter.
dns	Shows the DNS default domain name.
ecn-compatability	Shows the status of Explicit Congestion Notification (ECN) compatibility, either enabled or disabled.
force-msg	Shows the message control force message pattern settings.
mgid-usage	Shows the multicast group ID (MGID) usage for VLANs and multicast traffic.
msg-control	Shows the system message control function status (activated or disabled).
mtu	Shows system maximum transmission unit (MTU) information.
power	Shows power information for the chassis. Command options are: • **`global`**—power management settings • **`power-supply`**—power information for each power supply • **`slot`**—power information for each slot
setting	Shows system settings.
software	Shows the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags.
stats	Shows system statistics. For more information about statistics, see *Avaya Virtual Services Platform 9000 Performance Management, NN46250-701*.
topology-ip	Shows the circuitless IP set.

Default

None

Command mode

Privileged EXEC mode

show sys power

View power information for the chassis.

Syntax

show sys power [global]

show sys power [power-supply]

show sys power [slot]

Parameters

Variable	Value
global	Shows a summary of the power redundancy settings.
power-supply	Shows detailed power information for each power supply.
slot	Shows detailed power information for each slot.

Default

None

Command mode

Privileged EXEC mode

show sys-info

Displays the system status and technical information on the hardware components of the switch.

Syntax

show sys-info

show sys-info asic

show sys-info card

show sys-info fan

show sys-info power

show sys-info temperature

Parameters

Parameter	Description
asic	Specifies information about the application-specific integrated circuit (ASIC) installed on each module.
card	Specifies information about all the installed modules, including cooling modules, and firmware for the CF devices.
fan	Specifies information about installed cooling modules.
power	Specifies information about installed power supplies.
temperature	Specifies information about temperature.

Default

None

Command mode

Privileged EXEC mode

show tech

Display technical information about the status of the system and complete information about the hardware components, software components, and operation of the system.

Syntax

`show tech`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show telnet-access

Show the maximum number of Telnet sessions.

Syntax

show telnet-access

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show unsupported-lastset

Displays the last set of masked commands in the release.

Syntax

show unsupported-lastset

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show users

Display a list of users who are logged on to the system.

Syntax

show users

Parameters

None

Default

None

Command mode

Privileged EXEC mode

shutdown (for the management port)

Disable the Ethernet management port on the CP module.

Syntax

shutdown [port {slot/port[-slot/port][,...]}]

default shutdown [port {slot/port[-slot/port][,...]}]

no shutdown [port {slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port to disable the management port. The slots available are 1 and 2 in the format 1/2 or 2/1.

Default

The default is enabled.

Command mode

mgmtEthernet Interface Configuration mode

slpp (globally)

Enable the SLPP globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

Syntax

slpp enable

slpp tx-interval <500–5000>

slpp vid <1–4084>

default slpp

default slpp enable

default slpp tx-interval

no slpp

no slpp enable

no slpp vid <1–4084>

Parameters

Variable	Value
enable	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets.
tx-interval <*500–5000*>	Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500–5000..
vid <*1–4084*>	Adds a VLAN, by VLAN ID, to a SLPP transmission list.

Default

The default operation is disabled. The default interval is 500.

Command mode

Global Configuration mode

slpp (on a VLAN)

Enable the SLPP globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

Syntax

slpp enable

slpp tx-interval <500–5000>

slpp vid <1–4084>

default slpp

default slpp enable

default slpp tx-interval

no slpp

no slpp enable

no slpp vid <1–4084>

Parameters

Variable	Value
enable	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets.
tx-interval <*500–5000*>	Configures the SLPP packet transmit interval, expressed in milliseconds, in a range from 500–5000..
vid <*1–408*>	Adds a VLAN, by VLAN ID, to a SLPP transmission list.

Default

The default operation is disabled. The default interval is 500.

Command mode

VLAN Interface Configuration mode

slpp port

Enable SLPP by port to detect a loop and automatically stop it.

Syntax

slpp port {slot/port[-slot/port][,...]} packet-rx [packet-rx-threshold <1-500>]

default slpp port {slot/port[-slot/port][,...]} [packet-rx] [packet-rx-threshold]

no slpp port {slot/port[-slot/port][,...]} [packet-rx]

Parameters

Variable	Value
packet-rx	Enables or disables SLPP packet reception on the port.
packet-rx-threshold <*1-500*>	Specifies the SLPP reception threshold on the ports, expressed as an integer. The packet reception threshold specifies the

Variable	Value
	number of SLPP packets the port receives before it is administratively disabled. **Caution:** Avaya recommends that you configure the rx-threshold above 50 ms only on lightly loaded switches. If you configure the rx-threshold to a value greater than 50 ms on a heavily loaded switch and a loop occurs, the system can experience high CPU utilization.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default operation is disabled. The default threshold is 1.

Command mode

GigabitEthernet Interface Configuration mode

source

Source a configuration to merge a script file into the running configuration.

Warning:
You are not able to source a complete configuration file to merge it with your running configuration because the system can crash. The source command can be used to merge smaller portions of a configuration into the existing configuration.

Syntax

`source WORD<1–99> [debug] [stop] [syntax]`

Parameters

Variable	Value
debug	Debugs the script output.
stop	Stops the merge after an error occurs.
syntax	Verifies the script syntax.
WORD<1–99>	Specifies a filename and location in one of the following formats:

Variable	Value
	• a.b.c.d:<file> • peer:<file> • /intflash/<file> • /extflash/<file> • /usb/<file> The path and <file> can use 1–99 characters.

Default

None

Command mode

Privileged EXEC mode

speed (for the management port)

Configure the speed for the Ethernet management (mgmt) port on the CP module.

Syntax

`speed <10|100|port {slot/port[-slot/port][,...]}>`

`default speed [port {slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
<10|100>	Configures the connection speed for ports to 10 Mb/s or 100 Mb/s.
port*{slot/port[-slot/port][,...]}*	Identifies the slot and port to configure the speed for the ethernet management port. Slots available are 1 and 2.

Default

The default is 10 Mb/s.

Command mode

mgmtEthernet Interface Configuration mode

ssh (configuration)

Modifies Secure Shell (SSH) configuration parameters to support public and private key encryption connections.

Syntax

ssh

ssh dsa-auth

ssh dsa-host-key <512-1024>

ssh dsa-user-key WORD<1-15> [size <512-4096>]

ssh max-sessions <0-8>

ssh pass-auth

ssh port <1-65535>

ssh rsa-auth

ssh rsa-host-key [<512-1024>]

ssh secure

ssh timeout <1-120>

ssh version <both|v2only>

default ssh

default ssh dsa-auth

default ssh max-sessions

default ssh pass-auth

default ssh port

default ssh rsa-auth

default ssh secure

default ssh timeout

default ssh version

no ssh

no ssh dsa-auth

no ssh dsa-host-key <512-1024>

no ssh dsa-user-key WORD<1-15> [size <512-4096>]

no ssh pass-auth

no ssh rsa-auth

no ssh rsa-host-key [<512-1024>]

no ssh secure

Parameters

Variable	Value
dsa-auth	Enable or disable the DSA authentication.
dsa-host-key *<512–1024>*	Generates a new SSH DSA host key. The range of the host key size is 512 to 1024.
dsa-user-key *WORD<1–15> [size <512–4096>]*	Creates the DSA user key file. *WORD<1–15>* specifies the user access level. The valid user access levels for the Virtual Services Platform 9000 are: • rwa—Specifies read-write-all. • rw—Specifies read-write. • ro—Specifies read-only • rwl3—Specifies read-write for Layer 3. • rwl2—Specifies rread-write for Layer 2. • rwl1—Specifies read-write for Layer 1. *size <512–4096>* specifies the key size. The default is 1024 bits.
max-sessions *<0-8>*	The maximum number of SSH sessions allowed. A value from 0 to 8. Default is 4.
pass-auth	Enables password authentication.
port *<1-65535>*	Sets the SSH connection port. *<1-65535>* is the port number. The default is 22 **Important:** You cannot configure the following TCP ports as SSH connection ports: Ports 0 to 1024 (except port 22),1100, 4095, 5000, 5111, 6000, or 999.
rsa-auth	Enable RSA authentication.
rsa-host-key *<512–1024>*	Generates new SSH RSA host key. The range of the SSH host key size is 512 to 1024.
secure	Enables SSH in secure mode and immediately disables the access services SNMP, FTP, TFTP, rlogin, and Telnet.
timeout *<1-120>*	The SSH connection authentication timeout in seconds. Default is 60 seconds.

Variable	Value
version <*v2only*|*both*>	Sets the SSH version. Default is v2only. **Important:** Avaya recommends setting the version to v2 only.

Default

The default SSH version is 2.

Command mode

Global Configuration mode

ssh (connection)

Connects to a remote SSH host

Syntax

ssh WORD<1–256> -l WORD<1–32> [-p <1-32768>]

Parameters

Variable	Value
WORD<1–256>	Specifies the IP address or host name.
-l *WORD<1–32>*	Specifies the login name of the remote SSH server.
-p *<1-32768>*	Specifies the remote SSH server port number to which to connect. The default is 22.

Default

None

Command mode

Privileged EXEC mode

sys action

Reset system functions to reset all statistics counters, the console port, and the operation of the switchover function.

Syntax

sys action <cpu-switch-over|reset {console|counters}>

Parameters

Variable	Value
cpu-switch-over	Resets the switch to change over to the backup CPU.
reset {console|counters}	Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console connection stops responding. Resets all the statistics counters in the switch to zero. Resets the console port.

Default

None

Command mode

Privileged EXEC mode

sys clipId-topology-ip

Configures the circuitless IP (CLIP) ID as the topology IP.

Syntax

sys clipId-topology-ip <1–256>

Parameters

Variable	Value
<1–256>	Specifies the CLIP interface ID.

Default

None.

Command mode

Global Configuration mode

sys ecn-compatibility

Enable explicit congestion notification.

Syntax

sys ecn-compatibility

default sys ecn-compatibility

no sys ecn-compatibility

Parameters

Variable	Value
ecn-compatibility	Activates explicit congestion notification, as defined in Experimental Request For Comments (RFC) 2780. Virtual Services Platform 9000 does not currently support this feature.

Default

None

Command mode

Global Configuration mode

sys force-topology-ip-flag

Activates or disables the flag that configures the CLIP ID as the topology IP.

Syntax

sys force-topology-ip-flag enable

default sys force-topology-ip-flag [enable]

no sys force-topology-ip-flag [enable]

Parameters

None.

Default

The default is disabled.

Command mode

Global Configuration mode

sys mtu

Enable support for jumbo frames on Virtual Services Platform 9000.

Syntax

sys mtu <1522–9600>

default sys mtu

Parameters

Variable	Value
<1522–9600>	Activates Jumbo frame support for the data path. The value can be either 1522, 1950, or 9600 bytes. 1950 or 9600 bytes activate Jumbo frame support.

Default

The default value is 1950.

Command mode

Global Configuration mode

sys power

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity. Configure the slot priority to determine which slots shut down if insufficient power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first).

Syntax

sys power [fan-check]

sys power [slot {slot[-slot][,...]}]

sys power [slot-priority {<3–12>|SF2|SF3|SF5|SF6} {critical|high|low}]

default sys power [fan-check]

default sys power [slot {slot[-slot][,...]}]

default sys power [slot-priority {<3–12>|SF2|SF3|SF5|SF6}]

no sys power [fan-check]

no sys power [slot {slot[-slot][,...]}]

Parameters

Variable	Value
fan-check	Enables fan check to check the power management on the port.
slot {slot[-slot][,...]}	Enables power for a specific slot. Identify the slot in one of the following formats: a single slot (3), a range of slots (3-6), or a series of slots (3,5,6). The valid slots are: 1–12, SF1–SF6, or all.
slot-priority *{<3–12>|SF2|SF3|SF5|SF6} {critical|high|low}*	Designates the slot priority. You can configure priority for the interface module slots (3–12) or for Switch Fabric slots 2, 3, 5, and 6.

Default

Power management is enabled by default. The following list provides the default values for the applicable command parameters:

- fan-check: enable
- slot: enabled
- slot-priority: high

Command mode

Global Configuration mode

sys shutdown

Use this command to prepare the system for shutdown. This command properly shuts down the file system, and powers off all interface modules and Switch Fabric modules. The power supplies, cooling modules, and CP modules remain in the powered on state. After you use this command, you must physically turn off the chassis power.

To restore power after you use this command, you must physically turn the chassis power on again.

Syntax

`sys shutdown`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

telnet

Use this command to access the platform remotely.

Syntax

`telnet [WORD<1–256>]`

Parameters

Variable	Value
WORD <1–256>	Specifies the host name, IPv4 address or IPv6 address.

Default

None

Command mode

Privileged EXEC mode

telnet-access sessions

Configure the number of supported inbound Telnet sessions.

Syntax

`telnet-access sessions <0–8>`

`default telnet-access sessions`

Parameters

Variable	Value
<0–8>	Configures the allowable number of inbound Telnet sessions.

Default

The default is 8.

Command mode

Global Configuration mode

terminal

Configure the ACLI display.

Syntax

terminal length <8–64>

terminal length default

terminal more <enable|disable>

Parameters

Variable	Value
length *<8–64>*	Configures the number of lines in the output display for the current session.
length default	Configures the number of lines in the output display for the current session to the default value.
more <enable|disable>	Configures scrolling for the output display.

Default

The default length is 23 lines. The default for scrolling is enabled.

Command mode

Global Configuration mode

udp checksum

Enable the User Datagram Protocol (UDP) checksum calculation on the Virtual Services Platform 9000.

Syntax

udp checksum

default udp checksum

no udp checksum

Parameters

None

Default

The default is enabled.

Command mode

Global Configuration mode

udpsrc-by-vip

Enable virtual IP as the UDP source on the Virtual Services Platform 9000.

Syntax

udpsrc-by-vip

default udpsrc-by-vip

no udpsrc-by-vip

Parameters

None

Default

The default is enabled.

Command mode

Global Configuration mode

usb-stop

Stops the usb access and is done before removing the usb device.

Syntax

usb-stop

Parameters

None

Default

None

Command mode

Privileged EXEC mode

vsptalk

Create VSP Talk application.

Syntax

vsptalk

no vsptalk

Parameters

None

Default

Disabled

Command mode

Application mode

vsptalk add-buddy

Add your contact email to become a contact to receive and send messages through Instant Messaging.

Syntax

vsptalk <avaya|gtalk> client add-buddy WORD<0–1024>

no vsptalk <avaya|gtalk> client add-buddy WORD<0–1024>

Parameters

Variable	Value
<*avaya*|*gtalk*>	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: • avaya — Avaya XMPP IM • gtalk — Google Talk

Variable	Value
	Note: VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
<*avaya*|*gtalk*>client add-buddy *WORD<0–200>*	Adds your contact email to become a contact to receive and send messages through instant messaging. *WORD<0–200>* specifies your email address for the IM client. For instance, if you use Google Talk as the VSP Talk IM client your address is a gmail address: administrator1@gmail.com. The maximum number of contacts is 12.

Default

None

Command mode

Application mode

vsptalk client

Enable one of the instant messaging client types.

Syntax

`vsptalk <avaya|gtalk>`

`no vsptalk <avaya|gtalk>`

Parameters

Variable	Value
<*avaya*|*gtalk*>	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: • avaya — Avaya XMPP IM • gtalk — Google Talk **Note:** VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.

Default

The default is disabled.

Command mode

Application mode

vsptalk client username password

Define the VSP Talk instant messaging client username and password.

Syntax

vsptalk <avaya|gtalk> client username WORD<0–64> password WORD<0–80>

no vsptalk <avaya|gtalk> client username

Parameters

Variable	Value
<avaya|gtalk>	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: • avaya — Avaya XMPP IM • gtalk — Google Talk **Note:** VSP Talk uses only one client type at a time. You cannot use more than one client type simultaneously.
*<avaya|gtalk>*client username *WORD<0–64>* password *WORD<0–80>*	Defines the VSP Talk instant messaging client username and password. *WORD<0–64>* specifies the username and *WORD<0–80>* specifies the password. The username for Virtual Services Platform 9000 is the email used for Virtual Services Platform 9000 in the IM client.

Default

None

Command mode

Application mode

vsptalk enable

Enable the VSP Talk application.

Syntax

vsptalk <avaya|gtalk> enable

default vsptalk <avaya|gtalk> enable

no vsptalk <avaya|gtalk> enable

Parameters

Variable	Value
<*avaya*|*gtalk*|> enable	Enables VSP Talk to monitor the health and status of Virtual Services Platform 9000.

Default

The default is disabled.

Command mode

Application mode

vsptalk endpoint-address

Assign a VSP Talk endpoint address.

Syntax

vsptalk endpoint-address {A.B.C.D}

vsptalk endpoint-address {A.B.C.D} vrf WORD<0–16>

no vsptalk endpoint-address

Parameters

Variable	Value
{A.B.C.D}	Assigns an address for the VSP Talk application to use for communication. Virtual Services Platform 9000 supports IPv4 addresses for the VSP Talk feature.

Variable	Value
	To insulate mission critical applications, assign an address within your network that is separate from mission critical applications and other features.
vrf <*WORD<0–16>*	Specifies the name of the virtual router for which the endpoint address belongs. This is an optional parameter.

Default

None

Command mode

Application mode

vsptalk event-notification enable

Configure the IPv6 address for the Ethernet management port.

Syntax

`vsptalk event-notification enable`

`default vsptalk event-notification`

`no vsptalk event-notification`

Parameters

Variable	Value
event-notification enable	Enables event notification to receive instant messages on status updates or to allow Virtual Services Platform 9000 to notify you about alarm conditions. **Note:** In IM chat, you must also use the command **`enable event-notification`**.

Default

The default is disabled.

Command mode

Application mode

vsptalk server address

Specify the instant messaging server address.

Syntax

vsptalk <avaya|gtalk> server address WORD<0–255>

Parameters

Variable	Value
address *<0–255>*	Specifies the instant messaging server address.

Default

None

Command mode

Application mode

vsptalk server port

Configure encryption on the server.

Syntax

vsptalk <avaya|gtalk> server port <0–49151>

default vsptalk <avaya|gtalk> server port

Parameters

Variable	Value
port *<1–49151>*	Specifies the TCP port for instant messaging.

Default

The default port for avaya and gtalk is 5222.

Command mode

Application mode

vsptalk server encryption

Configure encryption on the server.

Syntax

vsptalk <avaya|gtalk> server encryption as-requested

vsptalk <avaya|gtalk> server encryption required

default vsptalk <avaya|gtalk> server encryption

Parameters

Variable	Value
encryption <*as-requested*|*required*>	Specifies the encryption option.

Default

The default is required.

Command mode

Application mode

vsptalk server proxy

Enables or disables the boundary-router on the router interface.

Syntax

vsptalk <avaya|gtalk> server proxy WORD<0–255>

no vsptalk <avaya|gtalk> server proxy

Parameters

Variable	Value
<avaya|gtalk>	Enables one of the instant messaging client types on Virtual Services Platform 9000. VSP 9000 supports the following: • avaya — Avaya XMPP IM • gtalk — Google Talk

Variable	Value
	Note: VSP Talk can use only one client type at a time. You cannot use more than one client type simultaneously.
server proxy WORD<0–255>	Configures a server proxy to access the Internet from the network. **Note:** Currently only HTTP proxy is supported for the proxy operator. You cannot use HTTPS with the proxy operator.

Default

The default is disabled.

Command mode

Application mode

vsptalk server ssl type

Enable, restore to default, or disable the old-style Secure Sockets Layer (SSL) interface.

Syntax

vsptalk <avaya|gtalk> server ssltype old

default vsptalk <avaya|gtalk> server ssltype

no vsptalk <avaya|gtalk> server ssltype old

Parameters

Variable	Value
ssltype old	Enables the old-style Secure Socket Layer interface. SSL is a protocol used to encrypt and transmit private documents over the Internet. DEFAULT: disabled **Note:** The system supports only HTTP proxy for the proxy operator. You cannot use HTTPS with the proxy operator.

Default

The default is disabled.

Command mode

Application mode

Chapter 4: BGP services commands

This chapter describes Avaya Command Line Interface (ACLI) commands to configure Border Gateway Protocol (BGP) services for the Avaya Virtual Services Platform 9000.

aggregate-address

Adds or deletes an aggregate address in a BGP routing table.

Syntax

aggregate-address WORD <1–256> [as-set] [summary-only] [suppress-map WORD<0-1536>] [advertise-map WORD <0-1536>] [attribute-map WORD<0-1536>]

default aggregate-address WORD <1–256> [as-set] [summary-only] [suppress-map] [advertise-map] [attribute-map]

no aggregate-address WORD <1–256> [as-set] [summary-only] [suppress-map WORD<0-1536>] [advertise-map WORD <0-1536>] [attribute-map WORD<0-1536>]

Parameters

variable	Value
WORD <1–256>	Specifies the IPv4 or the IPv6 address and an integer value in the range of 1 to 256.
as-set	Enables autonomous system information.
advertise-map *WORD<0-1536>*	Specifies the route map name (any string length between 0 and 64 characters) for route advertisements.
attribute-map *WORD <0-1536>*	Specifies the route map name (string length between 0 and 64 characters).
summary-only	Enables the summarization of routes not included in routing updates. This parameter creates the aggregate route and suppresses advertisements of more specific routes to all neighbors. The default value is disable.

variable	Value
suppress-map *WORD<0-1536>*	Specifies the route map name (string length between 0 and 64 characters) for the suppressed route list.

Default

The default value is disable.

Command mode

BGP Router Configuration mode

auto-peer-restart enable

Enables the process that automatically restarts a connection to a BGP neighbor.

Syntax

auto-peer-restart enable

default auto-peer-restart [enable]

no auto-peer-restart [enable]

Parameters

Variable	Value
enable	Enables the process that automatically restarts a connection to a BGP neighbor.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

auto-summary

Summarize the networks based on class limits after BGP is enabled. (For example, Class A, B, C networks).

Syntax

auto-summary

default auto-summary

no auto-summary

Parameters

None

Default

The default value is enable.

Command mode

BGP Router Configuration mode

bgp

Configure the IP BGP configuration commands.

Syntax

bgp [aggregation enable|always-compare-med|client-to-client reflection|cluster-id <A.B.C.D>|confederation identifier<0-65535> peers WORD <0-255>| default local-preference<0-2147483647>| deterministic-med enable|multiple-paths <1–8>]

Parameters

Variable	Value
aggregation enable	Enables or disables the aggregation feature on this interface.
always-compare-med	Enables the comparison of the multiexit discriminator (MED) parameter for paths from neighbors in different autonomous systems. A path with a lower MED is preferred over a path with a higher MED. The default value is disable.
client-to-client reflection	Enables or disables route reflection between two route reflector clients. This option is applicable only if the route reflection value is set to enable. The default value is enable.
cluster-id *<A.B.C.D>*	Sets a cluster ID. This option is applicable only if the route reflection value is set to enable, and if multiple route reflectors are in a cluster. *<A.B.C.D>* is the cluster ID of the reflector router.
confederation identifier *<0-65535> peers WORD <0-255>*	Configures a BGP confederation. The default value is 0.

Variable	Value
	• **identifier <0-65535>** specifies the confederation identifier. • **peers WORD <0-255>** Lists adjoining ASs that are part of the confederation in the format (5500,65535,0,10,...,...).
default local-preference *<0-2147483647>*	Specifies the default value of the local preference attribute. The default value is 100. You cannot change the default value when BGP is enabled.
deterministic-med enable	Enables deterministic Multiexit Discriminator (MED). The default value is enable.
multiple-paths *<1-8>*	Sets the maximum number of equal-cost-paths that are available to a BGP router by limiting the number of equal-cost-paths that can be stored in the routing table. The default value is 1.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

comp-bestpath-med-confed

When enabled, compares multiexit discriminator (MED) attributes within a confederation.

Syntax

comp-bestpath-med-confed enable

default comp-bestpath-med-confed [enable]

no comp-bestpath-med-confed [enable]

Parameters

Variable	Value
enable	Enables and compares multiexit discriminator attributes within a BGP confederation.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

debug-screen

Displays debug messages on the console, or saves them in a log file.

Syntax

debug-screen <off|on>

default debug-screen

no debug-screen

Parameters

Variable	Value
<on|off>	Disable BGP screen logging (off) or enable BGP screen logging (on).

Default

The default value is off.

Command mode

BGP Router Configuration mode

default-information

Enables the advertisement of a default route to peers, if it is present in the routing table.

Syntax

default-information originate

default default-information originate

no default-information originate

Parameters

Variable	Value
originate	Enables the origination default route.

Default

The default value is disable.

Command mode

BGP Router Configuration mode

default-metric (for BGP)

Configures a value that is sent to a BGP neighbor to determine the cost of a route a neighbor is using.

Syntax

default-metric <-1-2147483647>

default default-metric

no default-metric [<-1-2147483647>]

Parameters

Variable	Value
<-1-2147483647>	Specifies the range of the default metric. A default metric value helps solve the problems associated with redistributing routes that have incompatible metrics.

Default

The default value is -1.

Command mode

BGP Router Configuration mode

flap-dampening

Enables route suppression for routes that flap on and off.

Syntax

flap-dampening enable

default flap-dampening [enable]

no flap-dampening [enable]

Parameters

Variable	Value
enable	Enables BGP flap-dampening.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

ibgp-report-import-rt

Configures BGP to advertise imported routes to an interior BGP (IBGP) peer. This command enables or disables the advertisement of nonBGP imported routes to other IBGP neighbors.

Syntax

`ibgp-report-import-rt enable`

`default ibgp-report-import-rt [enable]`

`no ibgp-report-import-rt [enable]`

Parameters

Variable	Value
enable	Enables advertisement of non BGP imported routes to other IBGP neighbors.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

ignore-illegal-rtrid

Overlook an illegal router id after enabling BGP.

Syntax

`ignore-illegal-rtrid enable`

default ignore-illegal-rtrid [enable]

no ignore-illegal-rtrid [enable]

Parameters

Variable	Value
enable	Enable or disable the acceptance of a connection from a peer that sends an open message using a router ID of 0 (zero).

Default

The default value is enable.

Command mode

BGP Router Configuration mode

ip as-list

Use an asynchronous (AS) path list to restrict the routing information a router learns or advertises to and from a neighbor. The AS path list acts as a filter that matches AS paths.

Syntax

ip as-list <1-1024> memberId <0-65535> <permit|deny> as-path WORD<0-1536>

Parameters

Variable	Value
as-list *<1-1024>*	Creates the specified AS-path list entry.
as-path *WORD <0-1536>*	Specifies an integer value between 0 and 1536 placed within " ."
memberId *<0-65535>*	Adds a regular expression entry to the specified AS-path list. It is an integer value between 0 and 65 535.
<permit|deny>	Permits or denies access for matching conditions.

Default

None

Command mode

Global Configuration mode

ip bgp apply redistribute

Configure a redistribute entry to announce routes of a certain source protocol type into the Border Gateway Protocol (BGP) domain, for example, static, Routing Information Protocol (RIP), or direct routes.

Syntax

ip bgp apply redistribute direct [vrf <WORD 0–16>] [vrf-src <WORD 0–16>]

ip bgp apply redistribute ospf [vrf <WORD 0–16>] [vrf-src <WORD 0–16>]

ip bgp apply redistribute rip [vrf <WORD 0–16>] [vrf-src <WORD 0–16>]

ip bgp apply redistribute static [vrf <WORD 0–16>] [vrf-src <WORD 0–16>]

ip bgp apply redistribute [vrf <WORD 0–16>]

Parameters

Variable	Value
redistribute vrf<*WORD 0–16*>	Applies BGP redistribute for a particular VRF. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.
direct vrf<*WORD 0–16*>	Configures and displays the BGP direct configuration for a particular VRF. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.
ospf vrf<*WORD 0–16*>	Configures and displays the BGP OSPF configuration for a particular VRF. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.
rip vrf<*WORD 0–16*>	Configures and displays the BGP RIP configuration for a particular VRF. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.
static vrf<*WORD 0–16*>	Configures and displays the BGP static configuration for a particular VRF. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.
vrf-src<*WORD 0–16*>	Applies redistribute for a VRF source. <*WORD 0–16*> specifies the VRF name in the range of 0 to 16 characters.

Default

None

Command mode

Privileged EXEC Mode

ip bgp neighbor (for a VRF)

Syntax

ip bgp neighbor <nbr_ipaddr|peer-group-name>

ip bgp neighbor <nbr_ipaddr|peer-group-name> advertisement-interval <5-120>

ip bgp neighbor <nbr_ipaddr|peer-group-name> allow-as-in <0-10>

ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override

ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate

ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop

ip bgp neighbor <nbr_ipaddr|peer-group-name> enable

ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map WORD<0-256>

ip bgp neighbor <nbr_ipaddr|peer-group-name> max-prefix <0-2147483647>

ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable

ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask WORD<1-100>

ip bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self

ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map WORD<0-256>

ip bgp neighbor <nbr_ipaddr|peer-group-name> peer-group WORD<0-1536>

ip bgp neighbor <nbr_ipaddr|peer-group-name> remote-as WORD<0–11>

ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable

ip bgp neighbor <nbr_ipaddr|peer-group-name> retry-interval <1-65535>

ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community

ip bgp neighbor <nbr_ipaddr|peer-group-name> [site-of-origin <0-65535> <0-2147483647>|site-of-origin {A.B.C.D} <0-65535>]

ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable

ip bgp neighbor <nbr_ipaddr|peer-group-name> timers <0-21845> <0-65535>

ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source {A.B.C.D}

ip bgp neighbor <nbr_ipaddr|peer-group-name> weight <0-65535>

default ip bgp neighbor <nbr_ipaddr|peer-group-name> advertisement-interval

default ip bgp neighbor <nbr_ipaddr|peer-group-name> allow-as-in

default ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override

default ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate

default ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop

default ip bgp neighbor <nbr_ipaddr|peer-group-name> enable

default ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map

default ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask

default bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self

default ip bgp neighbor <nbr_ipaddr|peer-group-name> max-prefix

default ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable

default ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask

default ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map

default ip bgp neighbor <nbr_ipaddr|peer-group-name> remote-as

default ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable

default ip bgp neighbor <nbr_ipaddr|peer-group-name> retry-interval

default ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community

default ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin

default ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable

default ip bgp neighbor <nbr_ipaddr|peer-group-name> timers

default ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source

default ip bgp neighbor <nbr_ipaddr|peer-group-name> weight

no ip bgp neighbor <nbr_ipaddr|peer-group-name> WORD<0–1536>

no ip bgp neighbor <nbr_ipaddr|peer-group-name> as-override

no ip bgp neighbor <nbr_ipaddr|peer-group-name> default-originate

no ip bgp neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop

no ip bgp neighbor <nbr_ipaddr|peer-group-name> enable

no ip bgp neighbor <nbr_ipaddr|peer-group-name> in-route-map

no ip bgp neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable

no ip bgp neighbor <nbr_ipaddr|peer-group-name> neighbor-debug-mask

no ip bgp neighbor <nbr_ipaddr|peer-group-name> next-hop-self

no ip bgp neighbor <nbr_ipaddr|peer-group-name> out-route-map

no ip bgp neighbor <nbr_ipaddr|peer-group-name> peer-group

no ip bgp neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable

no ip bgp neighbor <nbr_ipaddr|peer-group-name> send-community

no ip bgp neighbor <nbr_ipaddr|peer-group-name> site-of-origin

no ip bgp neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable

no ip bgp neighbor <nbr_ipaddr|peer-group-name> update-source

no ip bgp neighbor <nbr_ipaddr|peer-group-name>

Parameters

Variable	Value
advertisement-interval *<5–120>*	Specifies the IP BGP route advertisement interval.
allow-as-in *<0–10>*	Specifies the IP BGP neighbor allow-as-in.
as-override	Specifies the as-override.
default-originate	Specifies the default-originate.
ebgp-multihop	Specifies EBGP-multihop.
enable	Enables the command.
in-route-map *WORD<0–256>*	Specifies the in-route-map.

Variable	Value
max-prefix *<0-2147483647>*	Specifies the max-prefix.
MD5-authentication enable	Enables the MD5–authentication.
neighbor-debug-mask *WORD<1-100>*	Specifies the neighbor-debug-mask.
next-hop-self	Specifies the next-hop-self.
<nbr_ipaddr|peer-group-name>	Specifies the neighbor IP address or the neighbor group name.
out-route-map *WORD<0-256>*	Specifies the out-route-map.
peer-group *WORD<0-1536>*	Specifies the peer group.
remote-as *WORD<0–11>*	Specifies the remote-as.
remove-private-as enable	Enables the remote-private-as enable.
retry-interval *<1-65535>*	Specifies the retry-interval.
send-community	Specifies the send-community.
site-of-origin *<0-65535> <0-2147483647>*	Specifies the site-of-origin.
site-of-origin *{A.B.C.D} <0-65535>*	Specifies the site-of-origin.
timers *<0-21845> <0-65535>*	Specifies the timers.
update-source *{A.B.C.D}*	Specifies the update-source.
weight *<0-65535>*	Specifies the weight.

Default

None

Command mode

VRF Router Configuration mode

ip bgp neighbor password (for a VRF)

Specify the password for IP BGP.

Syntax

ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>

default ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>

no ip bgp neighbor password <nbr_ipaddr|peer-group-name> WORD<0-1536>

Parameters

Variable	Value
<nbr_ipaddr|peer-group-name>	Specifies the peer IP address or the peer group name.
password	Configures the IP BGP neighbor password.
WORD<0–1536>	Specifies a password for IP BGP.

Default

None

Command mode

VRF Router Configuration mode

ip bgp restart-bgp

Restart BGP for a particular peer.

Syntax

ip bgp restart-bgp

ip bgp restart-bgp neighbor WORD<0–1536>

ip bgp restart-bgp neighbor WORD<0–1536> soft-reconfiguration {in|out}

ip bgp restart-bgp neighbor WORD<0–1536> vrf WORD<0–16>

ip bgp restart-bgp vrf WORD<0–16>

ip bgp restart-bgp vrf WORD<0–16> soft-reconfiguration {in|out}

Parameters

Variable	Value
WORD<1–1536>	Specifies the neighbor IP address or the neighbor group name.
soft-configuration {in|out}	Enables or disables soft-reconfiguration. If peer soft-reconfiguration is enabled in the in-bound direction, the policy can be changed and routes can be re-learned without having to reset the BGP connection. Enabling soft-reconfiguration, using the in parameter, causes the system to store all BGP routes in

Variable	Value
	local memory. Even non-best routes will be stored if soft-configuration in is enabled. Setting the value to out forces the neighbor to send out all the updates to the remote neighbor without resetting the connection.
vrf*WORD<0–16>*	Applies the BGP configuration for a particular VRF.

Default

The default for soft-reconfiguration is: in

Command mode

Privileged EXEC mode

ip bgp stats-clear-counters

Clears the BGP configuration statistics.

Syntax

`ip bgp stats-clear-counters`

`ip bgp stats-clear-counters neighbor <nbr_ipaddr|peer-group-name>`

`ip bgp stats-clear-counters vrf WORD<0–16>`

Parameters

Variable	Value
neighbor <*nbr_ipaddress*|*peer-group-name*>	Clears the BGP configuration statistics for the peer IP address or the peer group name.
vrf *WORD<0–16>*	Clears the statistics for the BGP configuration for a particular VRF.

Default

None

Command mode

Privileged EXEC mode

ip community-list

Use community lists to specify permitted routes by using their BGP community. This list acts as a filter that matches communities or AS numbers

Syntax

ip community-list <1-1024> memberId <0-65535> <permit|deny> community-string WORD<0-256>

Parameters

Variable	Value
community-list *<1-1024>*	Creates the specified community list entry. *<1-1024>* specifies the list id.
community-string *WORD<0-256>*	It is an alphanumeric string value with a string length of 0 to 1536 characters. This string value is either an AS num:community-value or a well-known community string. Well known communities include: • internet • no-export • no-advertise • local-as (known as NO_EXPORT_SUBCONFED)
memberId *<0-65535>*	Adds an entry to the community list. *<0-65535>* is an integer value that represents the member ID in the community list.
<permit|deny>	Sets the access mode, which permits or denies access for matching conditions.

Default

None

Command mode

Global Configuration mode

ip extcommunity-list

Use community lists to specify permitted routes by BGP extended community attributes, including route targets and sites of origin (SOO). This list acts as a filter that matches route targets and SOO.

Syntax

ip extcommunity-list <1-1024> memberId <0-65535> rt <0-65536> <0-2147483647> [soo {<0-65535> <0-2147483647>|<A.B.C.D> <0-65535>}]

Parameters

Variable	Value
memberId *<0-65535>*	Specifies an integer value between 0 and 65535 that represents the member ID in the community list.
rt *<0-65536> <0-2147483647>* rt *<A.B.C.D> <0-65535>*	Specifies the route target in the format {AS number:assigned number} (that is, {0 to 65535}:{0 to 2147483647}) or {ipaddress:assigned number} (that is, {a.b.c.d}:{0 to 65535}).
soo *<0-65535> <0-2147483647>* soo *<A.B.C.D> <0-65535>*	Specifies the site of origin in the format {AS number:assigned number} (that is, {0 to 65535}:{0 to 2147483647}) or {ipaddress:assigned number} (that is, {a.b.c.d}:{0 to 65535}).

Default

None

Command mode

Global Configuration mode

neighbor (for BGP)

Use peers and peer groups to simplify BGP configuration and make updates more efficient.

Syntax

neighbor WORD<0-1536> [address-family ipv6|address-family vpn4]

neighbor WORD<0-1536> advertisement-interval <5–120>

neighbor WORD<0-1536> [default-ipv6–originate|default-originate]

neighbor WORD<0-1536> ebgp-multihop

neighbor WORD<0-1536> enable

neighbor WORD<0-1536> [in-route-map WORD<0–256>|out-route-map WORD<0256>] [ipv6–in-route-map WORD <0–256>|ipv6–out-route-map WORD <0–256>]

neighbor WORD<0-1536> max-prefix <0–2147483647>

neighbor WORD<0-1536> MD5-authentication enable

neighbor WORD<0-1536> neighbor-debug mask WORD<1-100>

neighbor WORD<0-1536> next-hop-self

neighbor WORD<0-1536> peer-group WORD<0–1536>

neighbor WORD<0-1536> remote-as <0-65535>

neighbor WORD<0-1536> remove-private-as enable

neighbor WORD<0-1536>retry-interval <1-65535>

neighbor WORD<0-1536> route-reflector-client

neighbor WORD<0-1536> route-refresh

neighbor WORD<0-1536>send-community

neighbor WORD<0-1536>soft-reconfiguration-in enable

neighbor WORD<0-1536>timers <0–21845>

neighbor WORD<0-1536> update-source <A.B.C.D.>

neighbor WORD<0-1536> weight <0-65535>

default neighbor WORD<0-1536> [address-family ipv6|address-family vpn4]

default neighbor WORD<0-1536> advertisement-interval

default neighbor WORD<0-1536> [default-ipv6–originate|default-originate]

default neighbor WORD<0-1536> ebgp-multihop

default neighbor WORD<0-1536> enable

default neighbor WORD<0-1536> [in-route-map WORD<0–256>|out-route-map WORD<0256>] [ipv6–in-route-map WORD <0–256>|ipv6–out-route-map WORD <0–256>]

default neighbor WORD<0-1536> max-prefix

default neighbor WORD<0-1536> MD5-authentication enable

default neighbor WORD<0-1536> neighbor-debug mask WORD

default neighbor WORD<0-1536> next-hop-self

```
default neighbor WORD<0-1536> remote-as
default neighbor WORD<0-1536> remove-private-as enable
default neighbor WORD<0-1536>retry-interval
default neighbor WORD<0-1536> route-refresh
default neighbor WORD<0-1536>send-community
default neighbor WORD<0-1536> soft-reconfiguration-in enable
default neighbor WORD<0-1536> timers
default neighbor WORD<0-1536> update-source
default neighbor WORD<0-1536> weight
no neighbor WORD<0-1536>
no neighbor WORD<0-1536> [address-family ipv6|address-family vpn4]
no neighbor WORD<0-1536> [default-ipv6–originate|default-originate]
no neighbor WORD<0-1536> ebgp-multihop
no neighbor WORD<0-1536> enable
no neighbor WORD<0-1536> [in-route-map|out-route-map] [ipv6–in-
route-map|ipv6–out-route-map>]
no neighbor WORD<0-1536> MD5-authentication enable
no neighbor WORD<0-1536> neighbor-debug mask
no neighbor WORD<0-1536> next-hop-self
no neighbor WORD<0-1536> peer-group
no neighbor WORD<0-1536> remote-as
no neighbor WORD<0-1536> remove-private-as enable
no neighbor WORD<0-1536> route-reflector-client
no neighbor WORD<0-1536> route-refresh
no neighbor WORD<0-1536>send-community
no neighbor WORD<0-1536>soft-reconfiguration-in enable
no neighbor WORD<0-1536> update-source
no neighbor WORD<0-1536> weight
```

Parameters

Variable	Value
address-family <ipv6|vpnv4>	Enables BGP address families for IPv6 or IPv4 (BGP) and L3 VPN (MP-BGP) support. Enable this parameter for VPN/VRF Lite routes.
advertisement-interval *<5-120>*	Specifies the time interval (in seconds) that transpires between each transmission of an advertisement from a BGP neighbor. The default value is 5 seconds. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> advertisement-interval**.
default-originate	Enables the switch to send a default route advertisement to the specified neighbor. A default route does not have to be in the routing table. The default value is disable. Do not use this command if is globally enabled **default-information originate** The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> default-originate**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> default-originate**.
default-ipv6–originate	Enables IPv6 BGP neighbor default originate.
ebgp-multihop	Enables a connection to a BGP peer that is more than one hop away from the local router. The default value is disable. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> ebgp-multihop**.
enable	Enables the BGP neighbor. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> enable**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> enable**.
in-route-map *WORD<0-256>*	Applies a route policy rule to all incoming routes that are learned from, or sent to, the local BGP router peers, or peer groups. The local BGP router is the BGP router that

Variable	Value
	allows or disallows routes and sets attributes in incoming or outgoing updates. <*WORD 0-256*> name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> in-route-map WORD<0-256>**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> in-route-map**.
ipv6–in-route-map*WORD <0–256>*	Creates IPv6 in route map. Word <0–256> Specifies the route map name in the range of 0 to 256 characters.
ipv6–out-route-map*WORD <0–256>*	Creates IPv6 out route map. Word <0–256> Specifies the route map name in the range of 0 to 256 characters.
max-prefix *<0-2147483647>*	Sets a limit on the number of routes that can be accepted from a neighbor. The default value is 12000 routes. A value of 0 (zero) indicates that there is no limit to the number of routes that can be accepted. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> max-prefix**.
MD5-authentication enable	Enables TCP MD5 authentication between two peers. The default value is disable. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> MD5-authentication enable**.
neighbor-debug mask *WORD<1-100>*	Displays specified debug information for a BGP peer. The default value is none. *WORD<1-100>* is a list of mask choices separated by commas with no space between choices. For example, *{<mask>,<mask>,<mask>...}*. Mask choices are *none* disables all debug messages. *all* enables all debug messages. *error* enables display of debug error messages. *packet* enables display of debug packet messages. *event* enables display of debug event messages. *trace* enables display of debug trace messages. *warning* enables display of debug warning messages.

Variable	Value
	state enables display of debug state transition messages. *init* enables display of debug initialization messages. *filter* enables display of debug messages related to filtering. *update* enables display of debug messages related to sending and receiving updates. The default form of this command is **default neighbor <A.B.C.D|WORD 0-1536> neighbor-debug mask**.
next-hop-self	When enabled, specifies that the next-hop attribute in an IBGP update is the address of the local router or the router that is generating the IBGP update. The default value is disable. The next-hop parameter can only be configured when the neighbor is disabled. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> next-hop-self**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> next-hop-self**.
out-route-map *WORD<0-256>*	Applies a route policy rule to all outgoing routes that are learned from, or sent to, the local BGP router's peers, or peer groups. The local BGP router is the BGP router that allows or disallows routes and sets attributes in incoming or outgoing updates. *WORD<0-256>* name is an alphanumeric string length (0 to 256 characters) that indicates the name of the route map or policy. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> out-route-map <WORD 0-256>**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> out-route-map**.
peer-group *WORD<0-1536>*	Adds a BGP peer to the specified subscriber group. You must create the specified subscriber group before you issue this command. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> peer-group <WORD 0-1536>**.
remote-as *<0-65535>*	Configures the remote AS number of a BGP peer or a peer-group. You cannot configure this option when the admin-state is enable.

Variable	Value
	The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> remote-as**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> remote-as**.
remove-private-as enable	When enabled, strips private AS numbers when an update is sent. This feature is especially useful within a confederation. The default value is enable. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name>**.
retry-interval *<1-65535>*	Sets the time interval (in seconds) for the ConnectRetry Timer. The default value is 120 seconds. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> remove-private-as enable**.
route-reflector-client	Configures the specified neighbor or group of neighbors as its route reflector client. The default value is disable. All neighbors that are configured become members of the client group and the remaining IBGP peers become members of the nonclient group for the local route reflector. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> route-reflector-client**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> route-reflector-client**.
route-refresh	Enables IP VPN Route Refresh for the BGP peer. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> route-refresh**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> route-refresh**.

Variable	Value
send-community	Enables the switch to send the update message community attribute to the specified peer. The default value is disable. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> send-community**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> send-community**.
soft-reconfiguration-in enable	When enabled, the router relearns routes from the specified neighbor or group of neighbors without resetting the connection when the policy changes in the inbound direction. The default value is disable. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable**. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> soft-reconfiguration-in enable**.
timers <*0-21845*> <*0-65535*>	Sets timers (in seconds) for the BGP speaker for this peer. • <*0-21845*> is the keepalive time. • **<0-65535>** is the hold time. The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> timers**.
update-source <*A.B.C.D*>	Specifies the source IP address when BGP packets are sent to this peer or peer group. You cannot configure this parameter when the admin-state is enable. <*A.B.C.D*> is the specified source IP address. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> update-source <A.B.C.D>**.
weight <*0-65535*>	Specifies the weight of a BGP peer or peer groups, or the priority of updates that can be received from that BGP peer. The default value is 0. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor. The no form of this command is **no neighbor <nbr_ipaddr|peer-group-name> weight**.

Variable	Value
	The default form of this command is **default neighbor <nbr_ipaddr|peer-group-name> weight**.

Default

None

Command mode

BGP Router Configuration mode

neighbor password

Configure a BGP peer or peer group password for Transmission Control Protocol (TCP) MD5 authentication between two peers.

Syntax

neighbor password <nbr_ipadr|peer-group-name> WORD <0–1536>

default neighbor password <nbr_ipadr|peer-group-name> WORD <0–1536>

no neighbor password <nbr_ipadr|peer-group-name> WORD <0–1536>

Parameters

Variable	Value
password <nbr_ipadr|peer-group-name> *WORD <0–1536>*	Specifies a password for TCP MD5 authentication between two peers. *WORD <0–1536>* is an alphanumeric string length from 0 to 1536 characters.

Default

None

Command mode

BGP Router Configuration Mode

network (for BGP)

Specify the IGP network prefixes for BGP to advertise for redistribution.

Syntax

network WORD <1–256> [metric <0-65535>]

default network WORD <1–256>

no network WORD <1–256>

Parameters

Variable	Value
WORD <1–256>	Specifies IGP network prefixes for BGP to advertise for redistribution. This command imports routes into BGP.*Word <1–256>* is the IPv4 or the IPv6 network address and mask.
metric <*0-65535*>	metric <*0-65535*> corresponds to the multiexit discriminator (MED) BGP attribute for the route.

Default

None

Command mode

BGP Router Configuration mode

no-med-path-is-worst

Enable BGP to treat an update without a multiexit discriminator (MED) attribute as the worst path.

Syntax

no-med-path-is-worst enable

Parameters

Variable	Value
enable	Enables BGP to treat an update without a multiexit discriminator (MED) attribute as the worst path.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

quick-start

Enable the quick-start flag for exponential backoff.

Syntax

quick-start enable

default quick-start [enable]

no quick-start [enable]

Parameters

Variable	Value
enable	Enables the quick-start flag for exponential backoff.

Default

The default value is enable.

Command mode

BGP Router Configuration mode

redistribute (for BGP)

Enable redistribution to announce routes of a certain source protocol type into the BGP domain.

Syntax

redistribute <direct|ipv6–direct|ipv6–static|ospf|ospfv3|rip|static> [enable] [metric <0-65535>] [route-map WORD<0-64>] [vrf-src WORD<0-16>]

default redistribute <direct|ipv6–direct|ipv6–static|ospf|ospfv3|rip|static> [enable] [metric] [route-map]

no redistribute <direct|ipv6–direct|ipv6–static|ospf|ospfv3|rip|static> [enable] [route-map]

Parameters

Variable	Value
<direct|ipv6–direct|ipv6–static| ospf|ospfv3|rip|static>	Specifies the type of routes to redistribute to the BGP domain.
metric *<0-65535>*	Configures the metric to apply to redistributed routes.
route-map *WORD<0-64>*	Configures the route policy to apply to redistributed routes.
vrf-src *WORD<0-16>*	Specifies a VRF name. This parameter applies only to IPv4 routes.

Default

The default metric is 0.

Command mode

BGP Router Configuration mode

route-reflector enable

Enables the reflection of routes from IBGP neighbors.

Syntax

`route-reflector [enable]`

`default route-reflector [enable]`

`no route-reflector [enable]`

Parameters

None

Default

The default value is enable.

Command mode

BGP Router Configuration mode

route-refresh

Enables or disables IP VPN Route Refresh. If enabled, a route refresh request received by a BGP speaker causes the speaker to resend all route updates it contains in its database that are eligible for the peer that issues the request.

Syntax

`route-refresh`

`default route-refresh`

`no route-refresh`

Parameters

None

Default

The default value is disable

Command mode

BGP Router Configuration mode

router bgp

Access the router configuration mode to configure the Border Gateway Protocol (BGP) commands.

Syntax

`router bgp`

Note:

A separate command **`router bgp [WORD <0–11>] [enable]`** specifies the AS number and enables BGP.

Parameters

None

Default

None

Command mode

Global Configuration mode

router bgp as-4-byte enable

Globally enables 4–byte autonomous system numbers.

Syntax

router bgp as-4-byte enable

default router bgp as-4-byte enable

no router bgp as-4-byte enable

Parameters

None

Default

Disabled

Command mode

Global Configuration mode

router bgp as-dot enable

Globally enables the AS dot representation for 4–byte AS numbers.

Syntax

router bgp as-dot enable

default router bgp as-dot enable

no router bgp as-dot enable

Parameters

None

Default

Disabled

Command mode

Global Configuration mode

router bgp enable

Specifies the AS number and enable BGP.

Syntax

`router bgp [WORD <0–11>] [enable]`

Parameters

Variable	Value
enable	Enables the BGP on the router.
WORD<0–11>	Specifies the AS number. You cannot enable BGP until you change the local AS to a value other than 0.

Default

None

Command mode

Global Configuration mode

router bgp enable globally

Specify the AS number and enable BGP.

Syntax

`router bgp [WORD <0–11>][enable]`

Parameters

Variable	Value
enable	Enables the BGP on the router.
WORD<0–11>	Specifies the AS number. You cannot enable BGP until you change the local AS to a value other than 0.

Default

None

Command mode

Global Configuration mode

router-id (for BGP)

Specify the BGP router ID in IP address format. This parameter only applies to VRF 0.

Syntax

router-id <A.B.C.D>

default router-id

no router-id

Parameters

Variable	Value
<A.B.C.D>	Identifies the router IP address.

Default

None

Command mode

BGP Router Configuration mode

Show bgp ipv6 aggregates

Displays BGP IPv6 aggregates information.

Syntax

show bgp ipv6 aggregates [WORD <1-256>]

Parameters

Variable	Value
WORD <1-256>	Specifies IPv6 prefix and length in the range of 1 to 256

Default

None

Command mode

Privileged EXEC mode

Show bgp ipv6 imported-routes

Displays bgp ipv6 imported-routes information.

Syntax

show bgp ipv6 imported-routes [WORD <1-256>]

show bgp ipv6 imported-routes WORD <1-256> longer-prefixes

Parameters

Variable	Value
longer-prefixes	Shows long prefixes. the longer-prefixes indicate the mask length from a specified prefix to 32 (for example, show from prefix .B.C.D/len to A.B.C.D/32.)
WORD <1-256>	Specifies IPv6 prefix and length in the range of 1 to 256

Default

None

Command mode

Privileged EXEC mode

Show bgp ipv6 networks

Display information about BGP network configurations.

Syntax

show bgp ipv6 networks

show bgp ipv6 networks WORD <1–256>

Parameters

Variable	Value
WORD <1-256>	Specifies IPv6 prefix and length in the range of 1 to 256

Default

None

Command mode

Privileged EXEC mode

Show bgp ipv6 redistributed-routes

Display bgp ipv6 redistributed-routes information.

Syntax

show bgp ipv6 redistributed-routes

Parameters

None

Default

None

Command mode

Privileged EXEC mode

Show bgp ipv6 route

Display information about BGP IPv6 routes.

Syntax

show bgp ipv6 route

show bgp ipv6 route WORD <1–256>

show bgp ipv6 route community {disable|enable}

show bgp ipv6 route ipv6 WORD<1–256>

show bgp ipv6 route WORD<1–256> longer-prefixes

Parameters

Variable	Value
community *{disable|enable}*	Enables or disables the display of community attributes.
ipv6 *WORD<1–256>*	Specifies an IPv6 address.

Variable	Value
longer-prefixes	Shows long prefixes. the longer-prefixes indicate the mask length from any specified prefix to 32 (for example show from prefix A.B.C.D/len to A.B.C.D/32.)
WORD <1-256>	Specifies IPv6 address and length in the range of 1 to 256

Default

None

Command mode

Privileged EXEC mode

show ip as-list

Shows the AS path lists on the Global Router.

Syntax

show ip as-list [<1–1024>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<1–1024>	Specifies the list ID.
vrf *WORD<0-16>*	Specifies the name of the VRF.
vrfids *WORD<0–512>*	Specifies the VRF ID in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip bgp aggregates

Display information about current aggregate addresses.

Syntax

show ip bgp aggregates [<prefix/len>] [vrf WORD<0-16>] [vrfids WORD<0-255>]

Parameters

Variable	Value
<prefix/len>	Specifies the IP address and the mask length (the length can be 0 to 32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD <0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp cidr-only

Display information about classless interdomain routing (CIDR) routes.

Syntax

show ip bgp cidr-only [<prefix/len>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<prefix/len>	Specifies an exact match of the prefix. This is an IP address and an integer value between 0 and 32 in the format a.b.c.d/xx.
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp conf

View BGP configuration information on the switch.

Syntax

`show ip bgp conf [vrf WORD< 0–16>] [vrfids WORD< 0–512>]`

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp confederation

View BGP confederation information on the switch.

Syntax

`show ip bgp confederation`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip bgp dampened-paths

Display information about flap-dampened routes to determine unreliable routes.

Syntax

show ip bgp dampened-paths <A.B.C.D> [<prefix/len>] [longer-prefixes] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp flap-damp-config

Display global information about flap-dampening.

Syntax

show ip bgp flap-damp-config [<prefix/len>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
[<prefix/len>]	Exact match the prefix {a,b,c,d/len}.
vrf *WORD <0-16>*	Displays BGP configuration for a particular VRF.
vrfids *WORD<0-512>*	Specifies the VRF ID in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip bgp imported-routes

Display information about BGP imported routes.

Syntax

show ip bgp imported-routes [<prefix/len>] [longer-prefixes] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp neighbors

Display information about BGP peer advertised routes, peer routes, and IP VPN BGP peers.

Syntax

show ip bgp neighbors [{A.B.C.D}] [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip bgp neighbors [{A.B.C.D}] [advertised-routes] [<prefix/len>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip bgp neighbors {A.B.C.D} routes [<prefix/len>] [community <disable|enable>] [longer-prefixes] [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip bgp neighbors {A.B.C.D} stats [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip bgp neighbors {A.B.C.D} vpnv4 [<prefix/len>] [community <disable|enable>] [ext-community] [longer-prefixes] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
advertised-routes	Displays information about BGP peer advertised routes.
community	Enables the display of community attributes.
ext-community	Enables the display of extended community attributes.
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c.d/32).
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
routes	Displays information about BGP peer routes.
stats	Displays statistics information for BGP peers.
vpnv4	Displays information about IP VPN BGP peers.
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp networks

Display information about BGP network configurations.

Syntax

show ip bgp networks [<prefix/len>] [vrf WORD<0-16>] [vrfids WORD<0-255>]

Parameters

Variable	Value
<prefix/len>	Shows networks with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-255>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp peer-group

Display information about BGP peer groups.

Syntax

show ip bgp peer-group [WORD<0-1536>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
WORD<0-1536>	Specifies the name of the peer group.
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp vpnv4

Display information about IP VPN routes.

Syntax

show ip bgp vpnv4 [<prefix/len>] [longer-prefixes] [community] [ext-community] [ip {A.B.C.D}][vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
community	Enables the display of community attributes.
ext-community	Enables the display of extended community attributes.
ip *{A.B.C.D}*	Specifies the IP address.
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp redistributed-routes

View BGP redistribution information on the switch.

Syntax

show ip bgp redistributed-routes <prefix/len> vrf WORD<0–16> vrfids WORD<0–512>

Parameters

Variable	Value
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp route

Display information about BGP routes.

Syntax

show ip bgp route [<prefix/len>] [longer-prefixes] [community <enable|disable>] [ip <A.B.C.D>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<prefix/len>	Shows paths with this prefix. The prefix is the IP address and exact mask length (must be an integer value between 0 and 32).
community <enable|disable>	Enables or disables the display of community attributes.
ip *<A.B.C.D>*	Specifies an IP address.
longer-prefixes	Shows long prefixes. The longer-prefixes indicate the mask length from any specified prefix to 32 (for example, show from prefix a.b.c.d/len to a.b.c./32).
vrf *WORD<0-16>*	Specifies a VRF instance by name.

Variable	Value
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp summary

Display summarized information about BGP.

Syntax

`show ip bgp summary [vrf WORD<0-16>] [vrfids WORD<0-512>]`

Parameters

Variable	Value
vrf *WORD <0–16>*	Specifies a VRF instance by name.
vrfids *WORD <0–512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip bgp stats

View BGP statistics.

Syntax

`show ip bgp stats vrf WORD<0–16> vrfids WORD<0–512>`

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies a VRF instance by name.

Variable	Value
vrfids *WORD<0-512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show ip community-list

Shows the community lists on the Global Router.

Syntax

show ip community-list [<1–1024>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<1–1024>	Specifies the list ID.
vrf *WORD<0-16>*	Specifies the name of the VRF.
vrfids *WORD<0–512>*	Specifies the VRF ID in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

synchronization

Enable the router to accept routes from BGP peers without waiting for an update from the IGP.

Syntax

synchronization

default synchronization

no synchronization

Parameters

None

Default

The default value is enable.

Command mode

BGP Router Configuration mode

traps

Enable BGP traps.

Syntax

traps enable

default traps [enable]

no traps [enable]

Parameters

Variable	Value
enable	Enables BGP traps.

Default

The default value is disable.

Command mode

BGP Router and OSPF Router Configuration mode

Chapter 5: Commissioning commands

This chapter provides the Avaya Command Line Interface (ACLI) commands to commission the Avaya Virtual Services Platform 9000.

boot config host

Configure the remote host logon to modify parameters for FTP and TFTP access. Use the default parameters for TFTP transfers. If you want to use FTP as transfer mechanism, you must change the password to a valid value.

Syntax

boot config host {ftp-debug|password WORD<0–16>|tftp-debug|tftp-hash|tftp-rexmit <1–120>|tftp-timeout <1–120>|user WORD<0–16>}

default boot config host <ftp-debug|tftp-debug|tftp-hash|tftp-rexmit|tftp-timeout|user>

no boot config host <ftp-debug|tftp-debug|tftp-hash>

Parameters

Variable	Value
ftp-debug	Enables or disables the debug mode on FTP. If you enable the debug mode, debug messages appear on the management console screen.
password *WORD<0–16>*	Configures the password to enable FTP transfers. *WORD<0–16>* is the password, up to 16 characters. After you configure this password, you can use only FTP for remote host logon. **Important:** This password must match the password for the FTP server, or the FTP operation fails. Also, if you configure the password to a valid value, then all copying to and from the network uses FTP instead of TFTP. If the user name or password is incorrect, copying over the network fails.
tftp-debug	Enables or disables debug mode on TFTP or TFTPD. If you enable the debug mode, debug messages appear on the management console screen.
tftp-hash	Enables or disables the TFTP hash bucket display.

Variable	Value
tftp-rexmit <*1–120*>	Configures the TFTP retransmission timeout in seconds.
tftp-timeout <*1–120*>	Configures the TFTP timeout in seconds.
user *WORD<0–16>*	Configures the remote user logon. *WORD<0–16>* is the user logon name (up to 16 characters).

Default

The following list provides the command parameter defaults:

- ftp-debug: disabled
- tftp-debug: disabled
- tftp-hash: disabled
- tftp-rexmit: 2 seconds
- tftp-timeout: 6 seconds
- user: target

Command mode

Global Configuration mode

boot config master

Specify the primary CPU to determine which CPU you use as the master after the switch performs a full power cycle. After the CPU becomes the primary, the master LED for the CPU is on.

Syntax

`boot config master <1–2>`

Parameters

Variable	Value
<*1–2*>	Specifies the slot number for the master CPU. This variable can be 1 or 2. The default is slot 1.

Default

The default is slot 1.

Command mode

Global Configuration mode

cli password

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the Avaya Virtual Services Platform 9000, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Syntax

`cli password WORD<1–20> <layer1|layer2|layer3|read-only|read-write|read-write-all>`

Parameters

Variable	Value
WORD<1–20>	Specifies the user login name.
<layer1|layer2|layer3|read-only|read-write|read-write-all>	Changes the password for the specific access level.

Default

The following table provides the system default passwords.

Table 1: Access levels and default logon values

Access level	Default logon	Default password
Read-only	ro	ro
Layer 1 read/write	l1	l1
Layer 2 read/write	l2	l2
Layer 3 read/write	l3	l3
Read/write	rw	rw
Read/write/all	rwa	rwa

Command mode

Global Configuration mode

clock set

Configure the calendar time in the form of month, day, year, hour, minute, and second.

Syntax

clock set <MMddyyyyhhmmss>

Parameters

Variable	Value
<MMddyyyyhhmmss>	Specifies the month, day, year, hours, minutes, and seconds.

Default

None

Command mode

Privileged EXEC mode

clock time-zone

Configure the time zone to use an internal system clock to maintain accurate time. The time zone data in Linux includes daylight changes for all time zones from 1901 to 2038. You do not need to configure daylight savings.

Syntax

clock time-zone WORD<1–10> WORD<1–20> WORD<1–20>

default clock time-zone

no clock time-zone

Parameters

Variable	Value
WORD<1–10>	Specifies a directory name or a time zone name in /usr/share/zoneinfo, for example, Africa, Australia, Antarctica, or US. To see a list of options, enter clock time-zone at the command prompt without variables.
WORD<1–20> WORD<1–20>	The first instance of WORD<1–20> is the area within the timezone. The value represents a time zone data file in /usr/share/zoneinfo/WORD<1–10>/ , for example, Shanghai in Asia. The second instance of WORD<1–20>is the subarea. The value represents a time zone data file in /usr/share/zoneinfo/WORD<1–10>/

Variable	Value
	WORD<1–20>/, for example, Vevay in America/Indiana. To see a list of options, enter clock time-zone at the command prompt without variables.

Default

The default is Coordinated Universal Time (UTC).

Command mode

Global Configuration mode

ip address (for the management port)

Configure the IP address for the Ethernet management port.

Syntax

`ip address {A.B.C.D A.B.C.D|A.B.C.D/X}`

`no ip address {A.B.C.D}`

Parameters

Variable	Value
{A.B.C.D A.B.C.D|A.B.C.D/X}	Assigns an IP address and mask for the management port. **Important:** You cannot assign an address of 0.0.0.0/0. You can specify the mask in either dotted decimal notation or as a decimal number.

Default

None.

Command mode

mgmtEthernet Interface Configuration mode

ip route (for the management port)

Assign a static route to specify a gateway address route for the management interface. You can specify up to four static routes for the management interface.

Syntax

ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} weight <1–65535>

ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} preference <1–255>

ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} local-next-hop enable

ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} enable [next-hop-vrf WORD<0–16>]

default ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} [dynamic] [enable] [local-next-hop enable] [preference]

no ip route {A.B.C.D} {A.B.C.D} {A.B.C.D} [dynamic] [enable] [local-next-hop enable] [next-hop-vrf WORD<0–16>] [preference]

Parameters

Variable	Value
<1–65535>	Specifies the static route cost.
<1–255>	Indicates the route preference of this entry. If you can use more than one route to forward IP traffic, the switch uses the route with the highest preference. The higher the number, the higher the preference.
{A.B.C.D} {A.B.C.D} {A.B.C.D}	Specifies the IP address, subnet mask, and next-hop address for the route. The first {A.B.C.D} configures the destination IP address of this route. An entry with a value of 0.0.0.0 is the default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries depends on the network management protocol table access mechanisms. The second {A.B.C.D} configures the route network mask with the destination address before the switch compares the mask to the destination value. The third {A.B.C.D} configures the IP address of the next hop of this route. In the case of a route bound to an interface realized through a broadcast

Variable	Value
	media, the value of this box is the agent IP address on that interface.
WORD<0–16>	Specifies the VRF ID in inter-VRF static-route configuration.

Default

None

Command mode

MgmtRouter VRF Configuration mode

password

Configure password options.

Syntax

password [access-level WORD<2–8>] [aging-time day <1-365>] [default-lockout-time <60-65000>] [min-passwd-len <10-20>] [password-history <3-32>]

password lockout WORD<0–46> [time <60-65000>]

default password [access-level]

default password [aging-time] [default-lockout-time] [min-passwd-len] [password-history]

default password [lockout WORD<0–46> [time]]

no password {access-level WORD<2–8>|lockout WORD<0–46>}

Parameters

Variable	Value
access level *WORD<2–8>*	Permits or blocks this access level. The available access level values are as follows: • l1 • l2 • l3 • ro • rw • rwa

Variable	Value
aging-time day <*1-365*>	Configures the expiration period for passwords in days, from 1–365.
default-lockout-time <*60-65000*>	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60–65000 range.
lockout *WORD*<*0–46*> time <*60-65000*>	Configures the host lockout time. *WORD*<*0–46*> is the host IP address in the format a.b.c.d. <*60-65000*> is the lockout-out time, in seconds, in the 60–65000 range.
min-passwd-len <*10-20*>	Configures the minimum length for passwords in high-secure mode.
password-history <*3-32*>	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history.

Default

The following list provides the default values for the applicable command parameters:

- access level: allow all
- aging-time: 90 days
- default-lockout-time: 60 seconds
- lockout: 60 seconds
- min-passwd-len: 10 characters
- password-history: 3

Command mode

Global Configuration mode

save config

Saves the configuration to a file to retain the configuration settings.

Syntax

save config [file WORD<1–99>] [verbose] [standby WORD<1–99>] [backup WORD<1–99>]

Parameters

Variable	Value
backup*WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. *WORD<1–99>* uses one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file> /mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). The VSP supports /mnt/intflash and /mnt/extflash. *WORD<1–99>* is a string of 1–99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *WORD<1–99>* is a string of 1–99 characters.
standby *WORD<1–99>*	Saves the specified file name to the standby CPU in the following format:

Variable	Value
	• /intflash/ <file> • /extflash/ <file> • /usb/<file> *WORD<1–99>* is a string of 1–99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Default

None

Command mode

Privileged EXEC mode

show boot config master

View the current configuration for the master CPU.

Syntax

show boot config master

Parameters

None

Default

None

Command mode

Privileged EXEC mode

sys mgmt-virtual-ip

Assign an IP address to a virtual management port to use it for out-of-band (OOB) management. Create a virtual management port in addition to the physical management ports on the switch management modules.

Syntax

sys mgmt-virtual-ip {A.B.C.D/X|A.B.C.D A.B.C.D}

default sys mgmt-virtual-ip

no sys mgmt-virtual-ip

Parameters

Variable	Value
{A.B.C.D/X|A.B.C.D A.B.C.D}	Specifies the IP address and subnet mask in the format A.B.C.D/x or A.B.C.D/A.B.C.D. (For example, 10.127.231.15 255.255.255.0). **Important:** You cannot assign an address of 0.0.0.0/0.

Default

The default is no virtual IP address for the management port.

Command mode

Global Configuration mode

sys name

Configure system identification to specify the name of the switch.

Syntax

sys name WORD<0–255>

default sys name

Parameters

Variable	Value
name *WORD<0–255>*	Configures the system or root level prompt name for the switch. *WORD<0–255>* is an ASCII string from 1–255 characters (for example, LabSC7 or Closet4).

Default

The default is VSP-9012.

Command mode

Global Configuration mode

web-server

Enable the Web management interface to provide management access to the switch using a Web browser. Configure the TFTP server location of the Help files for the Web interface.

Syntax

web-server [def-display-rows <10–100>] enable [help-tftp WORD<0–256> <file>] [http-port <80–49151>] [secure-only]

web-server password {ro|rw|rwa} WORD<1–20> WORD<1–20>

default web-server [def-display-rows] enable [http-port]

no web-server enable

Parameters

Variable	Value
def-display-rows *<10–100>*	Configures the Web server default display row width.
enable	Enables the Web interface. You must enable the Web interface before you can connect to the system using Enterprise Device Manager (EDM).
help-tftp *WORD<0–256>*	Specifies the path to the TFTP server that stores the HTML Help files for the Web server. *WORD<0–256>* is a string of 0–256 characters. Specifies the file name in the following format: • a.b.c.d:/
http-port *<80–49151>*	Configures the Web server HTTP port.
password {ro|rw|rwa} *WORD<1–20> WORD<1–20>*	Specifies the username and the password for the access level. The access level can be read-only, read-write access, or read-write-all.
secure-only	Enables secure-only access to the web server. The default value for the secure-only option is enabled. By default the Web server is configured with the secure-only option, which

Variable	Value
	requires you to use https to access EDM. To access EDM using http, you must disable the secure-only option, by using: **no web-server secure-only**.

Default

The Web server is disabled, by default. The following list provides the default values for other command parameters:

- def-display-rows: 30
- http-port: 80
- https-port: 443
- secure-only: Enabled

Command mode

Global Configuration mode

show web-server

Displays the web server information.

Syntax

show web-server

Parameters

None

Default

None

Command mode

Privileged EXEC mode

Chapter 6: Ethernet modules commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to help you configure the Avaya Virtual Services Platform 9000 Ethernet modules.

auto-negotiate enable (on an Ethernet port)

Enable AutoNegotiation on the Ethernet port to optimally operate on the network.

Syntax

auto-negotiate [enable|port {slot/port[-slot/port][,...]}]

default auto-negotiate [enable|port {slot/port[-slot/port][,...]}]

no auto-negotiate [enable|port {slot/port[-slot/port][,...]}]

Parameters

Variable	Value
enable	Enables or disables AutoNegotiation for the port or other ports of the module or both.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is true, enabled.

Command mode

GigabitEthernet Interface Configuration mode

auto-negotiation-advertisements

Configure autonegotiation advertisements after you enable autonegotiation.

Syntax

auto-negotiation-advertisements [port {slot/port[-slot/port][,...]}] <10-full|10-half|100-full|100-half|1000-full|none>

default auto-negotiation-advertisements [port {slot/port[-slot/port][,...]}]

no auto-negotiation-advertisements [port {slot/port[-slot/port][,...]}]

Parameters

Variable	Value
10-full	Advertises 10 Mbps full duplex.
10-half	Advertises 10 Mbps half duplex.
100-full	Advertises 100 Mbps full duplex.
100-half	Advertises 100 Mbps half duplex.
1000-full	Advertises 1000 Mbps full duplex.
none	Configures the value to none.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

GigabitEthernet Interface Configuration mode

duplex

Configure the duplex mode on the Ethernet module. This command applies to 10/100/1000 Mb/s ports.

Syntax

duplex [port {slot/port[-slot/port][,...]}] <half|full>

default duplex [port {slot/port[-slot/port][,...]}] <half|full>

Parameters

Variable	Value
<half|full>	Specifies half- or full-duplex mode. 1 and 10 Gb/s ports must use full-duplex mode.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is half.

Command mode

GigabitEthernet Interface Configuration mode

lossless-port

Enable the lossless mode for the port.

Syntax

lossless-port enable

lossless-port pause-type {fc|pfc} [pfc-bandwidth <2–8>]

default lossless-port enable

default lossless-port pause-type

default lossless-port pfc-bandwidth

no lossless-port

Parameters

Variable	Value
enable	Enables Lossless Ethernet mode for the port. The default is disabled. Use the `no` parameter, `no lossless-port`, to disable Lossless Ethernet mode for the port. On Virtual Services Platform 9000, you can configure 10 GbE ports to be lossless. You can configure all unicast traffic on the port to be lossless, or you can configure all tagged unicast traffic with a specific lossless 802.1p value to be lossless. All tagged unicast traffic on the port with an

Variable	Value
	802.1p value matching the value of lossless-802.1p is lossless. The switch treats traffic that does not meet this requirement as lossy traffic. The switch can drop the lossy traffic. A maximum of two ports can be operational in a lossless cluster: either two lossless ports, or one lossless port and one lossy port. If a port in a cluster half is lossless enabled, the other three ports in that half will be held operationally down. If you do not enable Lossless Ethernet on any ports in a lossless cluster half, only the lowest numerical port, which is administratively enabled, is operational. The remaining three ports in the cluster half are operationally down. After you disable Lossless Ethernet on one half of a cluster, the system will allow one of the four ports in that half to be operationally up in lossy mode. After you disable Lossless Ethernet on the last port in a cluster, all eight ports return to the operational state prior to Lossless Ethernet configuration.
pause-type {fc|pfc}	Selects the pause frame type. • pause (FC) — All unicast traffic on the port is lossless. FC is the default pause type. • priority-based flow control (PFC) — All tagged unicast traffic on the port with an 802.1p value matching the value of lossless-802.1p is lossless. The switch treats traffic that does not meet this requirement as lossy traffic. The switch can drop the lossy traffic. The Lossless Ethernet feature applies to both directions on a lossless port. If the port becomes congested, the switch performs flow control based on the pause-type configuration. If traffic enters the device on a PFC-enabled port and exits the device on an FC-enabled port, only packets with the matching lossless-802.1 value are lossless. The following list identifies configuration limitations for Lossless Ethernet: • If you configure a port as lossless-PFC, it does not generate nor react to FC frames. • If you configure a port as lossless-FC, it does not generate nor react to PFC frames.
pfc-bandwidth *<2–8>*	Specifies the bandwidth in Gbps when the pause-type is set to pfc. The range is 2 to 8. **DEFAULT**: 5 Gbps

Default

The default for lossless-port enable is disabled.

The default pause-type is fc.

The default pfc-bandwidth is 5.

Command mode

GigabitEthernet Interface Configuration mode

name port

Specify the name of the port that needs to be changed and have same settings for all the ports.

Syntax

`name [port <portList>] WORD<0-42>`

Parameters

Variable	Value
portlist	Specifies the port number that needs to be changed.
WORD <0–42>	Specifies the new port name.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

qos lossless-802.1p

Configure the lossless 802.1p value.

The Lossless Ethernet feature for 10 GbE ports guarantees the switch does not drop certain traffic types.

You can configure all unicast traffic on the port to be lossless, or you can configure all tagged unicast traffic with a specific lossless-802.1p value to be lossless.

If you change the lossless-802.1p value, the change affects all priority-based flow control (PFC) configured ports.

You cannot change this value for individual lossless ports.

If traffic enters the device on a PFC-enabled port and exits the device on an FC-enabled port, only packets with the matching lossless-802.1p value are lossless.

Syntax

qos lossless-802.1p <0–6>

default qos lossless-802.1p

Parameters

Variable	Value
<0–6>	Specifies the lossless-802.1p value in a range from 0 to 6. **DEFAULT**: 3 **Note:** The following list identifies configuration limitations for the lossless-802.1p value: • Lossless-802.1p can be configured and the change affects all of the lossless-pfc ports in the system. The Lossless-802.1p value must be mapped to internal QoS level 3 and Avaya recommends that you do not use filters to remark the internal QoS. • When you enable lossless-PFC on a port, the port does not become lossless-PFC if the lossless-802.1p value is mapped to an internal QoS level other than 3, or if the internal QoS level 3 maps to another 802.1p value. • The system displays a warning message if at least one cluster is in Lossless-PFC mode, and you attempt to map a non-lossless 802.1p value to internal QoS level 3, or map the lossless 802.1p value to an internal QoS level other than 3. • You cannot change the Lossless 802.1p value to match the configured port QoS value on any of the Lossless-PFC enabled ports in the system. • You cannot enable Lossless-PFC on a port if the Lossless-PFC port QoS value is equal to the Lossless 802.1p value. On a Lossless-PFC enabled port, you cannot set the port QoS to a value which is the same as the Lossless 802.1p value." • In a Lossless-PFC (802.1Qbb) domain, the lossless behavior is guaranteed as long as the Lossless 802.1p, ingress "1p to QoS" map, and the egress "QoS to 1p" maps are consistent. You must configure the egress "QoS to 1p" map correctly when you change the Lossless 802.1p and Ingress "QoS to 1P" maps".

Default

The default is 3.

Command mode

Global Configuration mode

slot shutdown

Enable an Ethernet module to allow traffic to flow through it or disable an Ethernet module before you remove it from the chassis to minimize traffic loss. Traffic does not flow on a disabled module.

Syntax

`slot shutdown [port {slot/port[-slot/port][,...]}]`

`no slot shutdown [port {slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
<{slot/port[-slot/port][,...]}>	Identifies the slot and port numbers. Valid slot numbers are 3 to 12.

Default

None

Command mode

Global Configuration mode

show interface gigabitethernet config

Displays the Layer 3 trusted/untrusted information for a gigabitEthernet interface.

Syntax

`show interface gigabitEthernet config <1–4084> {slot/port[-slot/port][....]}`

Parameters

Variable	Value
1–4084	Specifies VLAN IDs as a value from 1 to 4084.
slot/port[-slot/port][....]	Specifies a port list.

Deafult

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet lossless-config

Display information on a port configured for Lossless Ethernet.

Syntax

show interfaces gigabitethernet lossless-config {slot/port [-slot/port][,...]}

Parameters

Variable	Value
lossless-config *{slot/port [-slot/port][,...]}*	Display information on a port configured for Lossless Ethernet. The parameter *{slot/port[-slot/port][,...]}* identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show qos lossless-802.1p

Displays the 802.1p value used for Lossless Ethernet.

Syntax

show qos lossless-802.1p

Parameters

None

Default

None

Command mode

Privileged EXEC mode

shutdown

Disable an Ethernet module before you remove it from the chassis to minimize traffic loss. Traffic does not flow on a disabled module.

Syntax

shutdown [port {slot/port[-slot/port][,...]}]

default shutdown [port {slot/port[-slot/port][,...]}]

no shutdown [port {slot/port[-slot/port][,...]}]

Parameters

Variable	Value
<{slot/port[-slot/port][,...]}>	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

GigabitEthernet Interface Configuration mode

speed

Set the speed of the port on the Ethernet modules.

Syntax

speed [port <portList>] <10|100|1000>

Parameters

Variable	Value
<10|100>	Specifies the port speed. Not applicable to 1 Gigabit or 10 Gigabit Ethernet modules.
port	Specifies the slot and the port number.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

tx-flow-control enable

Enable TX flow control to allow TX to transmit the MAC control PAUSE frames to indicate congestion on the receive side of the port interface. Flow control can only be enabled on 1 Gbit/s and 10 Gbit/s ports. Flow control cannot be enabled for ports that run at less than 1 Gbit/s.

Syntax

`tx-flow-control enable`

Parameters

Variable	Value
enable	Enables the TX flow control on the module.
port *[portlist]*	Specifies the slot and the port number.

Default

The default is disable.

Command mode

GigabitEthernet Interface Configuration mode

vrf

Associate a port to a Virtual Router Forwarding (VRF) so that the port becomes a member of the VRF instance.

Syntax

`vrf WORD<0-16>`

Parameters

Variable	Value
vrf *WORD<0-16>*	*WORD<0-16>* specifies the VRF name.

Default

None

Command mode

VLAN and GigabitEthernet Interface Configuration mode

Chapter 7: Fault management commands

This chapter provides information about fault management commands for the Virtual Services Platform 9000.

clear khi

Clear the forwarding health and CPP statistics information.

Syntax

clear khi forwarding [slot <3–12>]

clear khi cpp <iocop-statistics|port-statistics|protocoldrops>

Parameters

Variable	Value
slot *<3–12>*	Clears the forwarding health information for a particular interface module.

Default

None

Command mode

Privileged EXEC mode

show fulltech

Run all show commands and, optionally, capture the output to a file.

Syntax

show fulltech [file WORD<1–99>]

show fulltech khi [file WORD<1–99>]

Parameters

Variable	Value
file *WORD<1–99>*	Specifies the file name in the range of 1 to 99 for which you need the logs to be displayed. *WORD<1–99>* specifies the filename in the form /intflash/<file>| /extflash/<file>| /usb/<file>.

Default

None

Command mode

Privileged EXEC mode

show khi cpp

View key health information about the control processors.

Syntax

show khi cpp iocop-statistics [<3-12>]

show khi cpp port-statistics [{slot/port[-slot/port][,...]}]

show khi cpp protocol-drops

Parameters

Variable	Value
<3-12>	Specifies the slot number.
slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show khi forwarding

Displays forwarding health information on the switch.

Syntax

show khi forwarding <3–12>

show khi forwarding ifp <3–12>

show khi forwarding k2 <3–12>

show khi forwarding mac <3–12>

show khi forwarding mac-higig <3–12>

show khi forwarding qe <3–12>

show khi forwarding rsp <3–12>

show khi forwarding zagros <3–12>

Parameters

Variable	Value
<3–12>	Specifies the interface slot on the switch.
ifp *<3–12>*	Shows IFP statistics.
k2*<3–12>*	Shows K2 data path health indicators.
mac*<3–12>*	Shows MAC data path health indicators.
mac-higig*<3–12>*	Shows Mac-higig data path health indicators.
qe*<3–12>*	Shows QE2000 data path health indicators.
rsp*<3–12>*	Shows RSP data path health indicators.
zagros*<3–12>*	Shows Zagros data path health indicators.

Default

None

Command mode

Privileged EXEC mode

show khi performance

View the performance of the various components of the switch by checking their key health indicators.

Syntax

`show khi performance [buffer-pool|cpu|memory|process|pthread|slabinfo] {slot [-slot] [,...]}`

Parameters

Variable	Value
buffer-pool *{slot [-slot] [,...]}*	Indicates khi of the buffer-pool on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
cpu *{slot [-slot] [,...]}*	Indicates khi of the CPU on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
memory*{slot [-slot] [,...]}*	Indicates khi of memory on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
process*{slot [-slot] [,...]}*	Indicates khi of the process on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
pthread*{slot [-slot] [,...]}*	Indicates khi of pthread on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.
slabinfo*{slot [-slot] [,...]}*	Indicates khi of the slab information on the switch. *{slot [-slot] [,...]}* specifies the slot number. Valid slots are 1 to 12, or SF1 to SF6, or all.

Default

None

Command mode

Privileged EXEC mode

Chapter 8: IP routing commands

This chapter provides the Avaya Command Line Interface (ACLI) commands to perform general IP routing operations on the Avaya Virtual Services Platform 9000.

clear ip arp interface

Clear the ARP timers.

Syntax

clear ip arp interface gigabitethernet {slot/port[-slot/port][,...]}

clear ip arp interface vlan <1–4084>

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

hash-calc getEcmpRoute

View the Equal Cost Multipath (ECMP) route calculated by the hash algorithm from a source IP address to a destination IP address as a description.

Syntax

hash-calc getECMPRoute src-ip {A.B.C.D} dest-ip {A.B.C.D/X}

Parameters

Variable	Value
dest-ip *{A.B.C.D/X}*	Specifies the destination address and mask. The source and destination addresses cannot have the same value.
getECMPRoute	View the Equal Cost Multipath (ECMP) route calculated by the hash algorithm from a source IP address to a destination IP address as a description.
src-ip *{A.B.C.D}*	Specifies the source address. The source and destination addresses cannot have the same value.

Default

None

Command mode

Privileged EXEC mode

ip address (loopback)

Configure a circuitless IP interface (CLIP) when you want to provide a virtual interface that is not associated with a physical port. You can use a CLIP interface to provide uninterrupted connectivity to your switch. You can configure a maximum of 256 CLIP interfaces on each device.

Syntax

ip address {A.B.C.D} {A.B.C.D}

ip address [<1–256>] {A.B.C.D/X} vrf WORD<0–16>

ip address {A.B.C.D/X}

no ip address [<1–256>] {A.B.C.D} vrf WORD<0–16>

no ip address {A.B.C.D}

Parameters

Variable	Value
<1–256>	Specifies the interface identification number for the circuitless IP (CLIP).
{A.B.C.D/X}	Specifies the IP address and subnet mask.

Variable	Value
{A.B.C.D}	Specifies the IP address.
[vrf WORD<*0–16*>]	Specifies an associated VRF by name.
no	Deletes the address for a particular VRF.

Default

None

Command mode

Loopback Interface Configuration mode

ip alternative-route (globally)

Enable the alternative route feature globally.

Syntax

`ip alternative-route`

`default ip alternative-route`

`no ip alternative-route`

Parameters

Variable	Value
alternative-route	Enables or disables the Alternative Route feature. The default value is enabled. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

Default

Enabled

Command mode

Global Configuration mode

ip alternative-route (on a VRF)

Enable the alternative route feature globally.

Syntax

ip alternative-route

default ip alternative-route

no ip alternative-route

Parameters

Variable	Value
alternative-route	Enables or disables the Alternative Route feature. The default value is enabled. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added.

Default

Enabled

Command mode

VRF Router Configuration mode

ip area (loopback)

Designate an area for the circuitless IP (CLIP) interface.

Syntax

ip area [<1–256>] {A.B.C.D} vrf WORD<0–16>

ip area {A.B.C.D}

default ip area <1–256>

default ip area vrf WORD<0–16>

default ip area

no ip area <1–256>

no ip area <1–256> vrf WORD<0–16>

no ip area

Parameters

Variable	Value
<*1–256*>	Specifies the interface identification number for the CLIP.
{A.B.C.D}	Specifies the IP address of the OSPF area that is associated with the CLIP.
vrf WORD<*0–16*>	Specifies an associated VRF by name.
default	Sets the loopback area for a particular VRF to the default value of none.
no	Deletes the loopback area for a particular VRF.

Default

None

Command mode

Loopback Interface Configuration mode

ip arp-proxy enable

Configure an ARP proxy to allow a router to answer a local ARP request for a remote destination.

Syntax

ip arp-proxy enable

Parameters

Variable	Value
enable	Enables the proxy Address Resolution Protocol.

Default

None

Command mode

Interface Configuration mode

ip arp-response

Enable Address Resolution Protocol (ARP) on the switch to allow a router to answer a local ARP request.

Syntax

ip arp-response

Parameters

None

Default

None

Command mode

Interface Configuration mode

ip dhcp-relay (on an interface)

Configures DHCP Relay on an interface.

Syntax

ip dhcp-relay [broadcast] [circuitId] [max-hop <1-16>] [min-sec <0-65535>] [mode <bootp|dhcp|bootp_dhcp>] [remoteId] [trusted]

ip dhcp-relay fwd-path {A.B.C.D} [disable] [vrid <1-255>]

ip dhcp-relay fwd-path {A.B.C.D} [enable] [vrid <1-255>]

ip dhcp-relay fwd-path {A.B.C.D} [mode <bootp|dhcp|bootp_dhcp>] [vrid <1-255>]

ip dhcp-relay fwd-path {A.B.C.D} [vrid <1-255>]

default ip dhcp-relay [broadcast] [circuitId] [max-hop] [min-sec] [mode] [remoteId] [trusted]

default ip dhcp-relay fwd-path {A.B.C.D} [mode] [vrid <1-255>]

no ip dhcp-relay [broadcast] [circuitId] [remoteId] [trusted]

Note:

The command **no ip dhcp-relay** disables DHCP Relay but does not delete the DHCP entry.

no ip dhcp-relay fwd-path {A.B.C.D} [vrid <1-255>]

Parameters

Variable	Value
{A.B.C.D}	Creates a forwarding path to the DHCP server with a mode and a state. A.B.C.D is the IP address of the server. The default IP address of the relay is the address of the interface. **Tip:** If the relay is a Virtual Router configured on this interface, you must set the vrid.
broadcast	Enables the device to send the server reply as a broadcast to the end station. After you disable this variable, the device sends the server reply as a unicast to the end station.
circuitId	Enables the device to insert the Option 82 Circuit ID into the packets sent to the server (enables DHCP Option 82).
max-hop <*1-16*>	Configures the maximum number of hops before a BootP/DHCP packet is discarded (1–16). The default is 4.
min-sec <*0-65535*>	Configures the minimum seconds count for DHCP. If the secs field in the BootP/DHCP packet header is greater than this value, the device relays or forwards the packet; otherwise, the packet is dropped (0– 65535). The default is 0 seconds.
mode <bootp|dhcp|bootp_dhcp>	Configures DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both.
remoteId	Enables the device to insert the Option 82 Remote ID into the packets sent to the server (enables DHCP Option 82).
trusted	Configures the circuit as trusted in an Option 82 context.
vrid <*1-255*>	Specifies the ID of the virtual router and is an integer from 1–255.

Default

The default configuration forwards both BootP and DHCP messages. DHCP Option 82 is disabled. When you enable circuitId and/or remoteId you enable DHCP Option 82.

Command mode

Interface Configuration mode

ip dhcp-relay fwd-path

Create the forwarding path from the client to the server.

Syntax

ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>

no ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D>

Parameters

Variable	Value
fwd-path *<A.B.C.D> <A.B.C.D>*	Configures the forwarding path from the client to the server. • **A.B.C.D** is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or DHCP. The relay can also be a VRRP address. • **A.B.C.D** is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.

Default

None

Command mode

Global Configuration mode

ip dhcp-relay fwd-path enable

Enable the forwarding path from the client to the server.

Syntax

ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D> enable

Parameters

Variable	Value
fwd-path <*A.B.C.D*> <*A.B.C.D*> enable	Enables DHCP relaying on the path from the IP address to the server. • **A.B.C.D** is the IP address configured on an interface (a locally configured IP address). • **A.B.C.D** is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network, the DHCP packet is broadcast out from the interface.
disable	Disables DHCP relaying on the path from the IP address to the server.

Default

The ip dhcp-relay fwd-path default state is disabled.

Command mode

Global Configuration mode

ip dhcp-relay fwd-path mode

Modify DHCP mode to forward BootP messages only, DHCP messages only, or both.

Syntax

ip dhcp-relay fwd-path <A.B.C.D> <A.B.C.D> mode <bootp|bootp-dhcp|dhcp>

Parameters

Variable	Value
fwd-path <*A.B.C.D*> <*A.B.C.D*> mode <bootp|bootp-dhcp|dhcp>	Modifies DHCP mode to forward BootP messages only, DHCP messages only, or both. The default is both. • **mode** is {bootp | bootp_dhcp | dhcp}.

Default

The default mode is both.

Command mode

Global Configuration mode

ip ecmp

Enable Equal cost multiplepath protocol (ECMP).

Syntax

`ip ecmp`

`no ip ecmp`

Parameters

Variable	Value
no	Disables ECMP. If the ECMP parameter is disabled, all existing ECMP routes are removed. When ECMP is enabled, all ECMP routes are re-added.

Default

The default is disabled.

Command mode

Global Configuration mode

Related commands

Variable	Value
pathlist-1*WORD<0-64>*	Configures one equal-cost path to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-2 *WORD<0-64>*	Configures up to two equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-3 *WORD <0-64>*	Configures up to three equal-cost paths to the same destination prefix. To remove the policy, enter a blank string.

Variable	Value
	To configure this parameter, you must globally enable ECMP.
pathlist-4 *WORD <0-64>*	Configures up to four equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-5*WORD<0-64>*	Configures up to five equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-6 *WORD<0-64>*	Configures up to six equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-7 *WORD<0-64>*	Configures up to seven equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
pathlist-8 *WORD<0-64>*	Configures up to eight equal-cost paths to the same destination prefix. To remove the policy, enter a blank string. To configure this parameter, you must globally enable ECMP.
max-path*<1-8>*	Configures the maximum number of ECMP paths.

ip ecmp path-list apply

Apply changes to all Equal Cost Multipath (ECMP) path-list configurations.

Syntax

ip ecmp path-list apply

ip ecmp path-list apply vrf WORD<0–16>

Parameters

Variable	Value
path-list apply	Apply changes to all ECMP path-list configurations.
vrf *WORD<0–16>*	Apply changes to all ECMP path-list configurations for a particular VRF.

Default

None

Command mode

Privileged EXEC mode

ip forward-protocol udp

Configure UDP protocols to determine which UDP broadcasts are forwarded

Syntax

`ip forward-protocol udp`

Parameters

Variable	Value
<1-65535> WORD/1-15 *<1–15>*	Creates a new UDP protocol. • *<1-65535>*WORD *<1–15>*is the UDP protocol name as a string.
[vrf WORD*<0-32>*]	The name of the VRF.
[vrfids *<0–255>*]	The ID of the VRF. The value is an integer between 0 and 255.

Default

None

Command mode

Global Configuration mode

ip forward-protocol udp portfwd

Configure a UDP port forward entry to add or remove a port forward entry.

Syntax

ip forward-protocol udp portfwd

Parameters

Variable	Value
<1-65535> <A.B.C.D>	Adds a UDP protocol port to the specified port forwarding list. • *1-65535* is a UDP protocol port in the range of 1 to 65535. • *A.B.C.D* is an IP address in a.b.c.d format. Use the **no** operator to remove a protocol port forwarding entry and IP address from the list: **no ip forward-protocol udp portfwd <1-65535> <A.B.C.D>** To set this option to the default value, use the **default** operator with this command.
[vrf WORD<0-32>]	The name of the VRF.
[vrfids <0-255>]	The ID of VRF and is an integer between 0 and 255.

Default

None

Command mode

Global Configuration mode

ip forward-protocol udp portfwdlist

Configure the UDP port forwarding list.

Syntax

ip forward-protocol udp portfwdlist <1-1000>

Parameters

Variable	Value
<1-1000>	Creates a UDP port forwarding list in the range of 1 to 1000.

Default

None

Command mode

Global Configuration mode

ip forward-protocol udp broadcastmask

Configures the broadcast mask on the IP forwarding list.

Syntax

ip forward-protocol udp broadcastmask <A.B.C.D> [maxttl <1–16>]

Parameters

Variable	Value
<A.B.C.D>	Sets the interface broadcast mask (the interface broadcast mask can be different from the interface mask). • *A.B.C.D* is an IP address in a.b.c.d format.
maxttl <*1–16*>	Specifies the maximum time to live for the interface.

Default

None

Command mode

VLAN Interface Configuration mode

ip forward-protocol udp maxttl

Set the maximum time to live.

Syntax

ip forward-protocol udp maxttl <1-16>

Parameters

Variable	Value
maxttl <1-16>	Sets the maximum time-to-live value (TTL) for the UDP broadcast forwarded by the interface. The range is 1 to 16.

Default

None

Command mode

VLAN Interface Configuration mode

ip icmp

Enables ICMP redirect and unreachable messages.

Syntax

ip icmp redirect

ip icmp unreachable

default ip icmp redirect

default ip icmp unreachable

no ip icmp redirect

no ip icmp unreachable

Parameters

Variable	Value
redirect	Enables the switch to send ICMP destination redirect messages.
unreachable	Enables the switch to send ICMP unreachable messages. When enabled, generates Internet Control Message Protocol (ICMP) network unreachable messages if the destination network is not reachable from this router. These messages help determine if the routing switch

Variable	Value
	is reachable over the network. The default is disabled.

Default

Disabled

Command mode

Global Configuration mode

ip irdp

Enable Router Discovery globally so that the switch supports Router Discovery.

Syntax

ip irdp enable

Parameters

Variable	Value
enable	Enables the router discovery protocol on the switch.

Default

None

Command mode

Global Configuration mode

ip irdp address

Configure ICMP Router Discovery to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers.

Syntax

ip irdp address <A.B.C.D>

default ip irdp address <A.B.C.D>

Parameters

Variable	Value
address *<A.B.C.D>*	Specifies the IP destination address use for broadcast or multicast router advertisements sent from the interface. The address is the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255. The default address is 255.255.255.255.

Default

None

Command mode

Interface Configuration mode

Related commands

Variable	Value
holdtime *<4-9000>*	Configures the lifetime for advertisements. The default form of this command is **`default ip irdp holdtime`**.
maxadvertinterval*<4-1800>*	Specifies the maximum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the router interface. The default is 600 seconds. The default form of this command is **`default ip irdp maxadvertinterval`**.
minadvertinterval *<3-1800>*	Specifies the minimum time (in seconds) that elapses between unsolicited broadcast or multicast router advertisement transmissions from the interface. The range is 3 seconds to maxadvertinterval. The default is 450 seconds. The default form of this command is **`default ip irdp minadvertinterval`**.
multicast	Specifies if multicast advertisements are sent. The no form of this command is **`no ip irdp multicast`**.
preference *<-2147483648-2147483647>*	Specifies the preference (a higher number indicates more preferred) of the address as a default router address relative to other router addresses on the same subnet The default is 0.

Variable	Value
	The default form of this command is **default ip irdp preference**.

ip ospf apply accept adv-rtr

Apply the OSPF accept policy change to accept external routes from a specified advertising route.

Syntax

ip ospf apply accept adv-rtr <A.B.C.D>

ip ospf apply accept adv-rtr <A.B.C.D> vrf WORD<0–16>

Parameters

Variable	Value
adv-rtr *<A.B.C.D>*	Specifies the advertising router IP address.
vrf *WORD<0–16>*	Specifies the configuration for a particular VRF. *WORD<0–16>* specifies the VRF name.

Default

None

Command mode

Privileged EXEC mode

ip ospf apply accept

Apply OSPF accept policy changes to allow the configuration changes in the policy to take effect in an OSPF Accept context (and to prevent the switch from attempting to apply the changes one by one after each configuration change).

Syntax

ip ospf apply accept [vrf WORD<0-16>]

Parameters

Variable	Value
apply	Commits entered changes. Issue this command after modifying any policy configuration that affects an OSPF accept policy.
[vrf WORD<0-16>]	The name of the VRF.

Default

None

Command mode

Privileged EXEC mode

ip ospf (loopback)

Enable OSPF for the circuitless IP (CLIP) interface.

Syntax

ip ospf <1–256>

ip ospf vrf WORD<0–16>

ip ospf

default ip ospf <1–256>

default ip ospf vrf WORD<0–16>

default ip ospf

no ip ospf <1–256>

no ip ospf <1–256> vrf WORD<0–16>

no ip ospf

Parameters

Variable	Value
<1–256>	Specifies the interface identification number for the CLIP.
vrf WORD*<0–16>*	Specifies an associated VRF by name.
default	Sets the OSPF status on the loopback interface to the default of disabled.

Variable	Value
no	Disables the loopback OSPF for a particular value.

Default

The default is disabled.

Command mode

Loopback Interface Configuration mode

ip pim (loopback)

Enable PIM for the circuitless IP (CLIP) interface.

Syntax

ip pim bsr-candidate preference <0–255>

ip pim <1–256>

ip pim

default ip pim bsr-candidate

default ip pim <1–256>

default ip pim

no ip pim bsr-candidate

no ip pim <1–256>

no ip pim

Parameters

Variable	Value
bsr-candidate preference	Enables the CLIP interface as a candidate bootstrap router and configure a preference value. The C-BSR with the highest BSR preference and address is the preferred BSR.
<0–255>	Specifies the preference value.
<1–256>	Specifies the interface ID.
default	Sets the BSR candidate to the default. The default is —1, which indicates that the current interface is not a C-BSR.

Variable	Value
no	Sets the BSR candidate to the default. The default is —1, which indicates that the current interface is not a C-BSR.

Default

The default is —1, which indicates that the current interface is not a C-BSR.

Command mode

Loopback Interface Configuration mode

ip prefix-list

Use prefix lists to allow or deny specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used.

Configure a prefix list and apply list to any IP route policy.

Syntax

`ip prefix-list WORD<1-64>`

Parameters

Variable	Value
<A.B.C.D/X> [<ge|le> <0-32>]	Adds a prefix entry to the prefix list. • *A.B.C.D/X* is the IP address and mask. • *<ge|le> <0-32>* Lower bound and higher bound mask lengths together can define a range of networks. Use the **no** operator to remove a prefix entry from the prefix list: **`no ip prefix-list WORD<1-64> <A.B.C.D/X>`**
name *WORD<1-64>*	Renames the specified prefix list. The name length is from 1 to 64 characters.

Default

None

Command mode

Global Configuration mode

ip redistribute enable

Configure and enable redistribution entries to allow a protocol to announce routes of a certain source type, for example, static, RIP, or direct.

Syntax

ip <rip|ospf|bgp> redistribute <ospf|bgp|static|direct|rip> enable [vrf-src WORD<0-16>]

Parameters

Variable	Value
enable [vrf-src *<vrf-name>]*	Enables the OSPF route redistribution instance.
<ospf|bgp|static|direct|rip>	Specifies the type of routes to redistribute—the protocol source.
vrf *WORD<0-16>*	Specifies the VRF instance.
vrfids *<0-255>*	Specifies a list of VRF IDs.
vrf-src *WORD<0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
apply [vrf-src*<vrf-name>]*	Applies the redistribution configuration.
metric <metric-value> [vrf-src *<vrf-name>]*	Configures the metric to apply to redistributed routes.
metric-type <type1|type2> [vrf-src*<vrf-name>]*	Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.
route-policy <policy-name> [vrf-src*<vrf-name>]*	Configures the route policy to apply to redistributed routes.
subnets <allow|suppress> [vrf-src*<vrf-name>]*	Allows or suppresses external subnet route advertisements when routes are redistributed into an OSPF domain.

ip route (globally)

Configure a black hole static route to the destination a router advertises to avoid routing loops when aggregating or injecting routes to other routers.

Syntax

ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 enable [next-hop-vrf WORD<0-16>]

Parameters

Variable	Value
{A.B.C.D}	The first and second <*A.B.C.D*> specify the IP address and mask for the route destination. 255.255.255.255 is the black hole route.
enable	Adds a static or default route to the router or VRF. The no form of this command is **no ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 enable**
local-next-hop enable	Enables the local next hop for this static route. The default form of this command is **default ip route <A.B.C.D> <A.B.C.D> <A.B.C.D> local-next-hop enable**. The no form of this command is **no ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 local-next-hop enable**

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
next-hop-vrf *WORD<0-16>*	Specifies the next-hop VRF instance by name. The default form of this command is **default ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 next-hop-vrf**

Variable	Value
	WORD<0-16> The no form of this command is **no ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 next-hop-vrf WORD<0-16>**
weight *<1-65535>*	Specifies the static route cost. The default form of this command is **default ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 weight**
preference *<1-255>*	Specifies the route preference. The default form of this command is **default ip route <A.B.C.D> <A.B.C.D> 255.255.255.255 preference**

ip route default

The default route specifies a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. This route has a prefix length of zero (RFC 1812). You can configure routing switches with a static default route, or they can learn it through a dynamic routing protocol.

To create a default static route, you configure the destination address and subnet mask to 0.0.0.0.

Syntax

ip route 0.0.0.0 0.0.0.0 <A.B.C.D> enable [next-hop-vrf WORD<0-16>]

Parameters

Variable	Value
<A.B.C.D>	*<A.B.C.D>* specifies the IP address of the next-hop router (the next router at which packets must arrive on this route).
enable	Adds a static or default route to the router or VRF. The no form of this command is **no ip route 0.0.0.0 0.0.0.0 <A.B.C.D> enable**

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
local-next-hop enable	Enables the local next hop for this static route. The default form of this command is **default ip route 0.0.0.0 0.0.0.0 <A.B.C.D> local-next-hop enable**. The no form of this command is **no ip route 0.0.0.0 0.0.0.0 <A.B.C.D> local-next-hop enable**
next-hop-vrf *WORD<0-16>*	Specifies the next-hop VRF instance by name. The default form of this command is **default ip route 0.0.0.0 0.0.0.0 <A.B.C.D> next-hop-vrf WORD<0-16>** The no form of this command is **no ip route 0.0.0.0 0.0.0.0 <A.B.C.D> next-hop-vrf WORD<0-16>**
weight *<1-65535>*	Specifies the static route cost. The default form of this command is **default ip route 0.0.0.0 0.0.0.0 <A.B.C.D> weight**
preference *<1-255>*	Specifies the route preference. The default form of this command is **default ip route 0.0.0.0 0.0.0.0 <A.B.C.D> preference**

ip route preference

Syntax

ip route preference protocol <static|ospf-intra|ospf-inter|ebgp|ibgp|rip|ospf-extern1|ospf-extern2|staticv6|ospfv3-intra|ospfv3-inter|ospfv3-extern1|ospfv3-extern2> <0-255>

Parameters

Variable	Value
protocol <static|ospf-intra|ospf-inter|ebgp|ibgp|rip|ospf-extern1|ospf-extern2|staticv6|ospfv3-intra|ospfv3-inter|ospfv3-extern1|ospfv3-extern2> *<0-255>*	Configures the preference value for the specified protocol. If two protocols have the same configured value, the default value is used. • The protocol must be one of the following: static, ospf-intra, ospf-inter, ebgp, ibgp, rip, ospf-extern1, ospf-extern2, staticv6, ospfv3-intra, ospfv3-inter, ospfv3-extern1, or ospfv3-extern2. • **<0-255>** configures the priority. 0 is reserved for local routes. The default is 7.
vrf *WORD<0-16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0-255>*	Specifies a VRF instance by VRF number.

Default

The default priority is 7.

Command mode

Global Configuration mode

ip routing

Enable IP forwarding (routing) on a global level so that the router supports routing. You can use the IP address of any router interface for IP-based network management.

Syntax

ip routing

Parameters

Variable	Value
routing	Enables IP routing.

Default

None

Command mode

Global Configuration mode

ip rsmlt

Configure Routed Split MultiLink Trunking (RSMLT) on an IPv4 or IPv6 VLAN interface.

Syntax

ip rsmlt [holddown-timer <0-3600>] [holdup-timer <0–3600|9999>]

default ip rsmlt [holddown-timer <0-3600>] [holdup-timer <0-3600|9999>]

no ip rsmlt

Parameters

Variable	Value
holddown-timer<*0-3600*>	Defines how long the RSMLT switch does not participate in Layer 3 forwarding. • <*0-3600*> is the timer value in seconds. Avaya recommends that you configure this value to be longer than the anticipated routing protocol convergence.
holdup-timer<*0–3600*|*9999*>	Defines how long the RSMLT switch maintains forwarding for its peer. • *0-3600* is the timer value in seconds. 9999 means infinity.

Default

The default holddown timer is 60. The default holdup timer is 180.

Command mode

VLAN Interface Configuration mode

ip rsmlt edge-support

Configure RSMLT-edge to store the RSMLT peer MAC/IP address-pair in its local config file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches. The configuration applies to both IPv4 and IPv6.

Syntax

ip rsmlt edge-support

default ip rsmlt edge-support

no ip rsmlt edge-support

Parameters

Variable	Value
edge-support	Enables RSMLT-edge support.

Default

The default is disabled.

Command mode

Global Configuration mode

ip ttl

Configure the IP routing protocol stack to specify which routing features the switch can use.

Syntax

ip ttl <1-255>

default ip ttl

no ip ttl

Parameters

Variable	Value
ttl<*1-255*>	Configures the default time-to-live (TTL) value for a routed packet. The TTL is the maximum number of seconds before a packet is discarded. The default value of 255 is used whenever a time is not supplied in the datagram header.

Default

The default value is 255.

Command mode

Global Configuration mode

Related commands

Variable	Value
max-routes-trap enable	Enables the switch to send a trap when the maximum number of routes is exceeded. The no form of this command is **no max-routes-trap enable**. The default form of this command is **default max-routes-trap enable**.
more-specific-non-local-route	Enables the more-specific-non-local-route feature. If enabled, the switch can enter a more-specific nonlocal route into the routing table. The default form of this command is **default ip more-specific-non-local-route** The no form of this command is **no ip more-specific-non-local-route**
routing	Enables routing. The no form of this command is **no ip routing**.
supernet	Enables or disables supernetting. If supernetting is globally enabled, the switch can learn routes with a route mask of less then eight bits. Routes with a mask length less than eight bits cannot have ECMP paths, even if the ECMP feature is globally enabled. The default form of this command is **default ip supernet**. The no form of this command is **no ip supernet**.

ip vrrp

Configure Virtual Router Redundancy Protocol (VRRP) on a port or a VLAN.

Syntax

ip vrrp <1-255> enable

no ip vrrp <1-255> enable

default ip vrrp <1-255> enable

Parameters

Variable	Value
enable	Enables VRRP on the interface.

Default

None

Command mode

VLAN and GigabitEthernet Interface Configuration mode

Related commands

Variable	Value
action {none|preempt}	Use the action choice option to manually override the hold-down timer and force preemption. • **none|preempt** can be set to preempt the timer or set to none to allow the timer to keep working. To set this option to the default value, use the **default** operator with this command.
address *<1-255>* *<A.B.C.D>*	Set the IP address of the VRRP interface that forwards packets to the virtual IP addresses associated with the virtual router. • **A.B.C.D** is the IP address of the master VRRP. Use the **no** operator to remove the IP address of the VRRP interface: **no ip vrrp address <1-255> <A.B.C.D>** To set this option to the default value, use the **default** operator with this command.
adver-int *<1-255>*	Sets the the time interval between sending VRRP advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all participating routers. The default is 1. To set this option to the default value, use the **default** operator with this command.
backup-master enable	Enables the VRRP backup master. This option is supported only on Split MultiLink Trunking (SMLT) ports. Use the **no** operator to disable the VRRP backup master: **no ip vrrp <1-255> backup-master enable** To set this option to the default value, use the **default** operator with this command. **Important:** Do not enable Backup Master if Critical IP is enabled.

Variable	Value
critical-ip-addr <*A.B.C.D*>	Sets the critical IP address for VRRP. • *A.B.C.D* is the IP address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
critical-ip enable	Enables the critical IP address option. Use the **no** operator to disable the critical IP address option: **no ip vrrp <1-255> critical-ip enable** To set this option to the default value, use the **default** operator with this command. **Important:** Do not enable Critical IP if Backup Master is enabled.
fast-adv enable	Enables the Fast Advertisement Interval. The default is disabled. Use the **no** operator to disable VRRP on the port: **no ip vrrp <1-255> fast-adv enable** To set this option to the default value, use the **default** operator with this command.
fast-adv-int <*200-1000*>	Sets the Fast Advertisement Interval, the time interval between sending VRRP advertisement messages. • *200-1000* is the range in milliseconds, and must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds. To set this option to the default value, use the **default** operator with this command.
holddown-timer<*0-21600*>	Modifies the behavior of the VRRP failover mechanism by allowing the router enough time to detect the Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) routes. • *0-21600* is the time interval (in seconds) a router is delayed when changing to master state. To set this option to the default value, use the **default** operator with this command.

Variable	Value
priority *<1-255>*	Sets the port VRRP priority. • *1-255* is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router. To set this option to the default value, use the **default** operator with this command.

loop-detect action

Configure the ARP loop detection when loop-detect is enabled.

Syntax

loop-detect [action {port-down|mac-discard}] [arp-detect]

Parameters

Variable	Value
action	Indicates the action that the switch takes: port-down|vlan-block|mac-discard.
arp-detect	Enables arp detect.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

monitor ports error

Monitor port error information.

Syntax

monitor ports error collision

monitor ports error collision from {slot/port [-slot/port][,...]}

monitor ports error main

monitor ports error main from {slot/port [-slot/port][,...]}

monitor ports error ospf

monitor ports error ospf from {slot/port [-slot/port][,...]}

monitor ports error verbose

monitor ports error verbose from {slot/port [-slot/port][,...]}

Parameters

Variable	Value
collision	Monitor port collision error information.
collision from *{slot/port [-slot/port][,...]}*	Monitor port collision error information on a particular slot and port or particular slots and ports.
main	Monitor port general error information.
main from*{slot/port [-slot/port][,...]}*	Monitor general error information on a particular slot and port or particular slots and ports.
ospf	Monitor ports general Open Shortest Path First (OSPF) information.
ospf from*{slot/port [-slot/port][,...]}*	Monitor ports general OSPF information on a particular slot and port or particular slots and ports.
verbose	Monitor port extended error information.
verbose *{slot/port [-slot/port][,...]}*	Monitor port extended error information on a particular slot and port or particular slots and ports.
{slot/port [-slot/port][,...]}	Specifies the slot and port

Default

None

Command mode

Privileged EXEC mode

ping-virtual-address

Ping a virtual address to test the connection.

Syntax

ping-virtual-address enable

ping-virtual-address enable vrf WORD<0-16>

ping-virtual-address

default ping-virtual-address enable

default ping-virtual-address enable vrf WORD<0-16>

default ping-virtual-address

no ping-virtual-address enable

no ping-virtual-address enable vrf WORD<0-16>

no ping-virtual-address

Parameters

Variable	Value
vrf *WORD <0–16>*	Specifies the virtual router and forwarder (VRF) name from 1–16 characters.

Default

None

Command mode

VRRP Router Configuration mode

route-map enable

Configure and enable a route policy so that the switch can control routes that certain packets can take.

Syntax

route-map WORD<1-64> <1-65535>

Parameters

Variable	Value
match as-path *WORD <0-256>*	If configured, the switch matches the as-path attribute of the Border Gateway Protocol (BGP) routes against the contents of the specified AS-lists. This field is used only for BGP routes and ignored for all other route types. *WORD<0-256>* specifies the list IDs of up to four AS-lists, separated by a comma.
match community *WORD<0-256>*	If configured, the switch matches the community attribute of the BGP routes against the contents of the specified

Variable	Value
	community lists. This field is used only for BGP routes and ignored for all other route types. *WORD<0-256>* specifies the list IDs of up to four defined community lists, separated by a comma.
match community-exact enable	When disabled, match community-exact results in a match when the community attribute of the BGP routes match any entry of any community-list specified in match-community. When enabled, match-community-exact results in a match when the community attribute of the BGP routes matches all of the entries of all the community lists specified in match-community. **enable** enables match community-exact.
match interface *WORD<0-259>*	If configured, the switch matches the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This field is used only for RIP routes and ignored for all other route types. *WORD <0–259>* specifies the name of up to four defined prefix lists, separated by a comma.
match metric *<0-65535>*	If configured, the switch matches the metric of the incoming advertisement or existing route against the specified value. If 0, this field is ignored. *0-65535* The default is 0.
match network *WORD<0-259>*	If configured, the switch matches the destination network against the contents of the specified prefix lists. *WORD<0-259>* specifies the name of up to four defined prefix lists, separated by a comma.
match next-hop *WORD<0-259>*	If configured, matches the next-hop IP address of the route against the contents of the specified prefix list. This field applies only to nonlocal routes. • *WORD<0-259>* specifies the name of up to four defined prefix lists, separated by a comma.
match protocol *WORD<0-40>*	If configured, matches the protocol through which the route is learned. *WORD<0-40>* is any|xxx, where xxx is local, OSPF, External BGP (EBGP), Internal BGP (IBGP), RIP, static, or any combination, in a string length 0 to 40.
match route-source *WORD<0-259>*	If configured, matches the next-hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types. *WORD<0-259>* specifies the name of up to four defined prefix lists, separated by a comma.

Variable	Value
match-route-type {any|local|internal|external|external-1|external-2}	Sets a specific route type to match (applies only to OSPF routes). *any*|*local*|*internal*|*external*|*external-1*|*external-2* specifies OSPF routes of the specified type only (External-1 or External-2). Any other value is ignored.
match tag *WORD<0-256>*	Specifies a list of tags used during the match criteria process. Contains one or more tag values. *WORD<0-256>* is a value from 0 to 256.
match [vrf *WORD<0-16>] [vrfids <0-511>]*	Sets a specific VRF to match (applies only to OSPF routes).
name *WORD<1-64>*	Renames a policy and changes the name field for all sequence numbers under the given policy.
<permit|deny>	Specifies the action to take when a permit or deny policy is selected for a specific route. Permit allows the route, deny ignores the route.
set as-path *WORD<0-256>*	If configured, the switch adds the AS number of the AS-list to the BGP routes that match this policy. • *WORD<0-256>* specifies the list ID of up to four defined AS-lists separated by a comma. Use the **no** operator to delete the AS number: **no set as-path WORD<0–256>**
set as-path-mode <tag|prepend>	Sets the AS path mode. Prepend is the default configuration. The switch prepends the AS number of the AS-list specified in set-as-path to the old as-path attribute of the BGP routes that match this policy.
set automatic-tag enable	Sets the tag automatically. Used for BGP routes only. Use the **no** operator to disable the tag: **no set automatic-tag enable**
set community *WORD<0-256>*	If configured, the switch adds the community number of the community list to the BGP routes that match this policy. • *WORD<0-256>* specifies the list ID of up to four defined community lists separated by a comma.
set community-mode <additive|none|unchanged>	Sets the community mode. • **additive**—the switch prepends the community number of the community list specified in set-community

Variable	Value
	to the old community path attribute of the BGP routes that match this policy. • **none**—the switch removes the community path attribute of the BGP routes that match this policy to the specified value.
set injectlist *WORD<0-1027>*	If configured, the switch replaces the destination network of the route that matches this policy with the contents of the specified prefix list. • *WORD/0-1027* specifies one prefix list by name.
set ip preference <*0-255*>	Setting the preference to a value greater than 0 specifies the route preference value to assign to the routes that match this policy. This applies to accept policies only. • *0-255* is the range you can assign to the routes. The default is 0. If the default is configured, the global preference value is used.
set local-preference <*0-65535*>	A value used during the route decision process in the BGP protocol. Applicable to BGP only.
set local-preference WORD <0–655356>	Matches the local preference, applicable to all protocols.
set mask <*A.B.C.D*>	If configured, sets the mask of the route that matches this policy. This applies only to RIP accept policies. • *A.B.C.D* is a valid contiguous IP mask.
set metric <*0-65535*>	If configured, sets the metric value for the route while announcing a redistribution. The default is 0. If the default is configured, the original cost of the route is advertised into OSPF; for RIP, the original cost of the route or default-import-metric is used.
set metric-type {type1|type2}	If configured, sets the metric type for the routes to announce into the OSPF domain that matches this policy. The default is type 2. This field is applicable only for OSPF announce policies.
set next-hop *WORD<1–256>*	Specifies the IP address of the next-hop router. Use the **no** operator to disable set next-hop: **`no set next-hop`** The parameter, *WORD<1–256>*, specifies the next hop IP address.
set nssa-pbit enable	Sets the not so stubby area (NSSA) translation P bit. Applicable to OSPF announce policies only. Use the no parameter to disable the NSSA translation P bit, `no set nssa-pbit`.

Variable	Value
set origin {igp|egp|incomplete}	If configured, the switch changes the origin path attribute of the BGP routes that match this policy to the specified value.
set origin-egp-as *<0-65535>*	Indicates the remote autonomous system number. Applicable to BGP only.
set tag *<0-65535>*	Sets the tag of the destination routing protocol. If not specified, the switch forwards the tag value in the source routing protocol. A value of 0 indicates that this parameter is not set.
set weight *<0-65535>*	The weight value for the routing table. For BGP, this value overrides the weight configured through NetworkTableEntry, FilterListWeight, or NeighborWeight. Used for BGP only. A value of 0 indicates that this parameter is not set.
WORD<1-64> <1-65535>	Creates a route policy with a policy name and a sequence number. • **WORD<1-64>** is the policy name. • **1-65535** is the sequence number.

Default

None

Command mode

Global Configuration mode

routing

Enables or disables routing capabilities on specified switch ports. The specified port can be part of a routed VLAN, while routing is disabled only on that port.

Syntax

routing [enable]

routing [port {slot/port[-slot/port][,...]}] [enable]

default routing [enable]

default routing [port {slot/port[-slot/port][,...]}] [enable]

no routing [enable]

no routing [port {slot/port[-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	Sets the IP routing to enable.
port {slot/port[-slot/port][,...]}	Specifies the port and the slot number to be changed.

Default

The default setting for routing is enabled.

Command mode

Gigabitethernet Interface Configuration mode

send-trap

Configures Virtual Router Redundancy Protocol (VRRP) notification control.

Syntax

send-trap [enable] [vrf WORD<0-16>]

default send-trap [enable] [vrf WORD<0-16>]

no send-trap [enable] [vrf WORD<0-16>]

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies the VRF name.

Default

Generation of SNMP traps for VRRP events is enabled.

Command mode

VRRP Router Configuration mode

show interfaces gigabitethernet loopback

Display the circuitless IP interface configuration information.

Syntax

show interfaces loopback vrf WORD<0-16> vrfids WORD<0-512>

Parameters

Variable	Value
vrf WORD<0-16>	Displays the loopback information for the associated VRF name. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters.
vrfids WORD<0-512>	Displays the loopback configuration for the specified VRF IDs. *WORD<0-512>* specifies the VRF IDs in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip arp

Show ARP information to view the configuration information in the ARP table.

Syntax

show ip arp [<A.B.C.D>] [-s <A.B.C.D>] [gigabitEthernet <slot/port>] [interface <gigabitethernet|vlan>] [spbm-tunnel-as-mac][static-mcastmac <-s | vrf | vrfids | <A.B.C.D>][vlan <1–4084>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<A.B.C.D>	The specific network IP address for the table.
-s *<A.B.C.D> <A.B.C.D>*	The specific subnet for the table.
gigabitEthernet	Displays the entries for a particular brouter port.
interface	Displays ARP interface configuration information.

Variable	Value
	Use the following parameters to display ARP table information specifically for: • gigabitEthernet {slot/port [-slot/port][,...]} displays IP ARP gigabitEthernet interface information • VLAN <1–4084> displays IP ARP VLAN interface information
static-mcastmac	Displays static multicast MAC ARP information. Use these parameters to display ARP table information specifically for multicast MAC ARP as follows: • -s {A.B.C.D/X} — the specific IP/subnet value • vrf WORD<0–16>— the static multicast MAC configurations for a particular VRF • vrfids WORD<0–512> — IP ARP static multicast MAC VRFIDS • {A.B.C.D} — specifies the network IP address
vlan	Displays ARP entries for a particular VLAN ID. Use these parameters to display ARP table information specifically for: • vrf WORD<0–16> — the VLAN VRF name • vrfids WORD<0–512> — the VLAN VRF ID
vrf *WORD<0-16>*	Specifies the name of the VRF. The total number of ARPs listed in the summary line of the **`show ip arp`** display represents the total number of ARPs on the chassis including all VRFs (which includes the Mgmt Router VRF).
vrfids *WORD<0–512>*	The VRF ID. The total number of ARPs listed in the summary line of the **`show ip arp`** display represents the total number of ARPs on the chassis, including all VRFs (which includes the Mgmt Router VRF).
{A.B.C.D}	Specifies the network IP address for the table.

Default

None

Command mode

Privileged EXEC mode

show ip arp interface

Show ARP port information to display data about the specified port, all ports, or the VLAN.

Syntax

show ip arp interface [vlan <1–4084>]

show ip arp interface gigabitethernet [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show ip dhcp-relay

Display relay information to show relay information about DHCP routes and counters.

Syntax

show ip dhcp-relay counters [option82] [vrf WORD<0-16>] [vrfids <0-512>]

show ip dhcp-relay fwd-path [vrf WORD<0-16>] [vrfids <0-512>]

show ip dhcp-relay interface gigabitethernet [{slot/port[-slot/port][,...]}][<1–4084>] [vrf WORD<0-16>] [vrfids <0-512>]

show ip dhcp-relay interface vlan [<1–4084>]

show ip dhcp-relay interface [vrf WORD<0-16>] [vrfids <0-512>]

Parameters

Variable	Value
counters	Displays the count of DHCP Relay requests and replies.
fwd-path	Displays information about DHCP Relay forward paths.
gigabitethernet {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
interface	Specifies the interface.
option82	Shows statistics for the relay agent option.
vlan *<1–4084>*	Specifies the VLAN ID.
vrf *WORD<0-16>*	Specifies the name of the VRF.
vrfids *<0-512>*	Specifies the ID of the VRF. The value is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip ecmp

Display the prefix list of routes with number of ECMP paths.

Syntax

show ip ecmp max-path

show ip ecmp pathlist-1 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-2 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-3 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-4 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-5 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-6 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-7 [vrf WORD<0-16>] [vrfids WORD<0-512>]

show ip ecmp pathlist-8 [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
max-path	Configures the maximum number of ECMP paths.
pathlist-1 *vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 1 ecmp path. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-2*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 2 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-3*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 3ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-4*vrf WORD <0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 4 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-5*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 5 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-6*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 6 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-7*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 7 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-8*vrf WORD<0-16> vrfids WORD<0-512>*	Displays prefix list of routes with 8 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.

Variable	Value
vrf *WORD<0-16>*	Displays the prefix list of routes with 1 ecmp path for a particular VRF. *WORD<0-16>* specifies the VRF name in the range of 0 to 32 characters.
vrfids *WORD<0-512>*	Displays the prefix list of routes with 1 ecmp path for a particular VRF ID. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

Related commands

Variable	Value
pathlist-2 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 2 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-3 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 3ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-4 WORD <0-16> vrfids WORD<0-512>	Displays prefix list of routes with 4 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-5 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 5 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-6 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 6 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-7 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 7 ecmp paths. *WORD<0-16>* specifies the VRF name in the range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.
pathlist-8 WORD<0-16> vrfids WORD<0-512>	Displays prefix list of routes with 8 ecmp paths. *WORD<0-16>* specifies the VRF name in the

Variable	Value
	range of 0 to 16 characters. *WORD<0-512>* specifies the VRF ID in the range of 0 to 512.

show ip extcommunity-list

Shows extended community list information.

Syntax

show ip extcommunity-list

show ip extcommunity-list <1–1024> vrf WORD<0–16>

show ip extcommunity-list <1–1024> vrfids WORD<0–512>

show ip extcommunity-list <1–1024>

show ip extcommunity-list vrf WORD<0–16>

show ip extcommunity-list WORD<0–512>

Parameters

Variable	Value
<1–1024>	Specifies the extended community list ID.
vrf *WORD<0–16>*	Displays extended community list for a particular VRF.
vrfids *WORD<0–512>*	Specifies VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip forward-protocol udp

Display the UDP protocol table with the UDP port numbers for each supported or designated protocol.

Syntax

show ip forward-protocol udp [vrf WORD<0-16>] [vrfids <0-512>]

Parameters

Variable	Value
interface <*A.B.C.D*>	Displays information about the UDP interface for all IP addresses or a specified IP address.
portfwd	Displays the UDP port forwarding table.
portfwdlist <*1–1000*>	Displays the UDP port forwarding list table for the specified list or all lists on the switch. <*1–1000*> specifies the port forward list ID.
vrf *WORD<0-16>*	Specifies the name of the VRF in the range of 0 to 16 characters.
vrfids <*0-512*>	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip forward-protocol udp portfwdlist

View and confirm the configuration setting on the IP forwarding list.

Syntax

show ip forward-protocol udp portfwdlist <1–1000> [vrf WORD<0-16>] [vrfids <0-512>]

Parameters

Variable	Value
<*1–1000*>	Specifies the port forward list id which is an integer in the range of 1 to 1000.
vrf *WORD<0-16>*	The name of the VRF in the range of 0 to 16 characters.
vrfids <*0-512*>	The ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Global Configuration mode

show ip forward-protocol udp portfwd

View and confirm the port forward entry configuration.

Syntax

show ip forward-protocol udp portfwd [vrf WORD<0-16>] [vrfids <0-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	The name of the VRF in the range of 0 to 16 characters.
vrfids *<0-512>*	The ID of VRF and is an integer between 0 and 512.

Default

None

Command mode

Privileged EXEC mode

show ip interface

Shows the IP configuration for an interface.

Syntax

show ip interface

show ip interface gigabitethernet [<1–4084>] [{slot/port[-slot/port][,...]}]

show ip interface [vrf WORD <0-16>] [vrfids WORD <0-512>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
vrf WORD*<0-16>*	Specifies the name of the VRF.
vrfids WORD *<0–512>*	Specifies the VRF ID in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip irdp

Confirm that the Router Discovery is enabled.

Syntax

show ip irdp

show ip irdp interface gigabitethernet [{slot/port[-slot/port][,...]}] [<1–4084>]

show ip irdp interface vlan [<1–4084>]

show ip irdp [vrf WORD<0–16>] [vrfids WORD<0–512>]

Parameters

Variable	Value
1–4084>	Specifies VLAN ID.
gigabitethernet *{slot/port[-slot/port][,...]}*	Shows ports route discovery information. *{slot/port[-slot/port][,...]}* specifies the port.
interface	Displays route discovery information for each interface type.
vlan *<1–4084>*	Shows VLAN route discovery information. *[1–4084>* specifies VLAN ID.

Variable	Value
vrf *WORD<0–16>*	Displays route discovery for a particular VRF.
vrfids *WORD<0–512>*	Displays route discovery for a particular VRF Ids.

None

Default

None

Command mode

Privileged EXEC mode

show ip prefix-list

Display the prefix list.

Syntax

show ip prefix-list [WORD<1-64>] [prefix <A.B.C.D>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
prefix *{A.B.C.D}*	Adds a prefix entry to the prefix list. *{A.B.C.D}* is the IP address.
WORD <1–64>	Renames the specified prefix list. The name length is from 1 to 64 characters.
vrf *WORD <0–16>*	Shows prefix list information for a particular VRF.
vrfids *WORD <0–512>*	Shows prefix list for particular VRF ids. The ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip route

Displays the IP route information.

Syntax

show ip route [<A.B.C.D>] [-s <A.B.C.D/X>] [-s default][alternative] [count-summary] [preference] [static] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<A.B.C.D>	Specifies the IP address of the route to the network.
-s default	Specifies the default subnet.
-s *<A.B.C.D/X>*	Indicates the IP address and subnet mask for which to display routes.
alternative	Displays the alternative routes.
count-summary	Displays ip route count summary.
preference	Displays the route preference information.
static	Shows static route information.
vrf *WORD<0-16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0-512>*	Specifies a VRF instance by VRF number.

Default

None

Command mode

Privileged EXEC mode

show ip route preference

Display the IP route preference information to confirm that the configuration is correct.

Syntax

show ip route preference [vrf WORD<0-16>] [vrfids WORD<0-255>]

Parameters

Variable	Value
`vrf WORD<0-16>`	Specifies a VRF instance by VRF name.
`vrfids WORD<0-255>`	Specifies a VRF instance by VRF number.

Default

None

Command mode

Global Configuration mode

show ip routing

Displays the ip routing configuration information.

Syntax

`show ip routing [vrf WORD<0–16>] [vrfids WORD<0–512>]`

Parameters

Variable	Value
vrf *WORD<0–16>*	Specifies a VRF by name in the range of 0 to 16 characters.
vrfids*WORD<0–512>*	Specifies a VRF id in the range of 0 to 512.

None

Default

None

Command mode

Privileged EXEC mode

show ip redistribute

Display and ensure the accuracy of the configuration settings.

Syntax

show ip <rip|ospf|bgp> redistribute [interface] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
<ospf|bgp|static|direct|rip>	Specifies the type of routes to redistribute—the protocol source.
vrf *WORD<0-16>*	Displays rip configuration for a particular VRF.
vrfids *WORD<0–512>*	Specifies a list of VRF IDs.
interface	Shows rip information for each interface.

Default

None

Command mode

Privileged EXEC mode

show ip rsmlt

Show IP RSMLT information to view data about all RSMLT interfaces.

Syntax

show ip rsmlt [<local|peer>] [vrf WORD<0–16>] [vrfids WORD<0–512>]

Parameters

Variable	Value
[<local|peer>]	Specifies values for the local or peer switch.
vrf *WORD<0–16>*	Displays IP routing for a VRF.
vrfids *WORD<0–512>*	Displays IP routing for a range of VRFs.

Default

None

Command mode

Privileged EXEC mode

show ip rsmlt edge-support

Display RSMLT-edge status information.

Syntax

show ip rsmlt edge-support

Parameters

Variable	Value
edge-support	Displays RSMLT edge support and peer information.

Default

None

Command mode

Privileged EXEC mode

show ip vrf

Use the following command to view VRF configurations.

Syntax

show ip vrf

show ip vrf max-routes [vrfids WORD <0–512>] [WORD <0–16>]

show ip vrf WORD <0–16>

show ip vrf vrfids WORD<0–512>

Parameters

Variable	Value
max-routes	Displays the maximum number of routes for the specifies VRFs.
WORD <0–16>	Specifies a VRF by name.
vrfids *WORD<0–512>*	Specifies a list of VRFs by VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp

Displays the global Virtual Router Redundancy Protocol (VRRP) configuration.

Syntax

show ip vrrp

show ip vrrp vrf WORD <0–16>

show ip vrrp vrfids WORD<0–512>

Parameters

Variable	Value
WORD <0–16>	Specifies a VRF by name.
vrfids *WORD<0–512>*	Specifies a list of VRFs by VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp address

Display basic VRRP configuration information about the specified port, all ports, or the VLAN.

Syntax

show ip vrrp address [addr {A.B.C.D}][vrid <1-255>] [addr <A.B.C.D>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
addr *{A.B.C.D}*	Specifies the IP address of the master VRRP.
vrf *WORD<0–16>*	Specifies the name of the VRF.
vrid *<1–255>*	Specifies a unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.
vrfids *WORD<0–512>*	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp interface gigabitEthernet

Display the VRRP interface gigabitEthernet configurations.

Syntax

show ip vrrp interface gigabitEthernet [{slot/port[-slot/port][,...]}] [1–4084>]

show ip vrrp interface gigabitEthernet verbose

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID in the range of 1 to 4084.
{slot/port[-slot/port][,...]}	Specifies the slot/port number of a range of ports.
verbose	Displays all available information about the VRRP interface gigabitEthernet configurations.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp interface

Display VRRP information about the interface.

Syntax

`show ip vrrp interface`

Parameters

Variable	Value
gigabitEthernet *{slot/port [-slot/port][,...]}*	Shows the VRRP interface gigabitEthernet configurations.
verbose	Shows all available information about the VRRP interfaces.
vlan <*1-4084*>	Specifies the VLAN that contains the VRRP. <*1-4084*> specifies the VLAN ID n the range of 1 to 4084.
vrf *WORD<0–16>*	Specifies a unique integer value that represents the virtual router ID in the range of 1–255. The virtual router acts as the default router for one or more assigned addresses.
vrfids *WORD<0–512>*	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp interface vlan

Show the extended VRRP configuration for all VLANs on the switch or for the specified VLAN.

Syntax

show ip vrrp interface vlan [<1-4084>] [verbose] [vrf WORD<0–16>] [vrfids WORD<0–512>][{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
vlan *<1-4084>*	The VLAN ID in the range of 1 to 4084.
{slot/port [-slot/port][,...]}	The slot/port number of a range of ports.
vrf *WORD<0–16>*	The name of the VRF.
vrfids *WORD<0–512>*	The ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Privileged EXEC mode

show route-map

Display current information about the IP route policy.

Syntax

show route-map detail [vrf WORD<0-16>] [vrfids WORD<0-512>]

show route-map [WORD <1-64>] [seq <1-65535>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
detail	Specifies the long format information of the route map.

Variable	Value
WORD<1-64> seq <1-65535>	Displays a route policy with a policy name and a sequence number. • **WORD<1-64>** is the policy name. • **seq <1-65535>** is the sequence number.
vrf *WORD<0-16>*	Specifies the name of the VRF.
vrfids *WORD<0–512>*	Specifies the ID of the VRF and is an integer in the range of 0 to 512.

Default

None

Command mode

Global Configuration mode

Chapter 9: IP multicast routing commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to configure multicast routing protocols that the Avaya Virtual Services Platform 9000 supports.

ip arp static-mcast

Configure Layer 3 multicast MAC filtering to route an IP frame to a unicast IP address and flood it with a destination multicast MAC address. You must manually define a static ARP entry that associates an IP address with a multicast MAC address, flooding ports, and a multilink trunk.

Syntax

ip arp static-mcast {A.B.C.D} <0x00:0x00:0x00:0x00:0x00:0x00> vid <1–4084> [port {slot/port[-slot/port][,...]}] [WORD<1–16>]

default ip arp static-mcast {A.B.C.D}

no ip arp static-mcast {A.B.C.D}

Parameters

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address in hexadecimal format. **Important:** The MAC address parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive).
vid*1–4084*	Specifies the VLAN ID.
A.B.C.D	Specifies the IP address.
{slot/port[-slot/port][,...]}	Specifies the port that receives the multicast flooding. Type the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
WORD<1–16>	Specifies the multilink trunk ID.

Default

None

Command mode

Global Configuration mode

Related Parameters

Variable	Value
request-threshold *<50–1000>*	Maximum number of outstanding unresolved ARP requests. The value ranges from 50 to 1000.
timeout *<1–32767>*	Sets the ARP lifetime aging period in minutes. The value ranges from 1 to 32767 minutes.
vid*1–4084*	Specifies the VLAN ID.
A.B.C.D *<0x00:0x00:0x00:0x00:0x00:0x00>* *{slot/port[-slot/port][,...]}* vid *<1–4084>*	*A.B.C.D* adds the ARP entries. *<0x00:0x00:0x00:0x00:0x00:0x00>* specifies the MAC address in hexadecimal format. *{slot/port[-slot/port][,...]}* specifies the slot and the port number to add the ARP entry. vid specifies the VLAN id in the range of 1 to 4084.

ip igmp

Configure the Internet Group Management Protocol (IGMP) commands to establish and manage the multicast groups.

Syntax

ip igmp generate-log

ip igmp generate-trap

ip igmp immediate-leave-mode <multiple-user|one-user>

ip igmp ssm [dynamic-learning] [group-range {A.B.C.D/X}]

ip igmp ssm-map all

ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]

default ip igmp ssm-map {A.B.C.D} {A.B.C.D}

default ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]

no ip igmp ssm-map {A.B.C.D} {A.B.C.D}

no ip igmp ssm-map {A.B.C.D} {A.B.C.D} [enable]

Parameters

Variable	Value
generate-log	Sets the IGMP log.
generate-trap	Sets the IGMP trap.
immediate-leave-mode <multiple-user|one-user	Enables immediate leave mode to users which is either a single user or multiple users.
ssm [dynamic-learning] [group-range {*A.B.C.D/X*}]	Enables and sets the Source Specific Multicast (SSM) features. The parameter, dynamic-learning enables SSM dynamic learning. The parameter, group range *{A.B.C.D/X}* configures the range group address and mask. The SSM range parameter extends the default SSM range of 232/8 to include an IP multicast address. You can configure existing applications without having to change their group configurations. This parameter specifies an IP multicast address within the range of 224.0.0.0 and 239.255.255.255. The default is 232.0.0.0. The address mask is the IP address mask of the multicast group. The default is 255.0.0.0.
ssm-map all	Enable the SSM map table for all static entries.
ssm-map*{A.B.C.D} {A.B.C.D}* [enable]	Enable the SSM map table for a specific entry or create a static entry for a specific group. The parameter, {A.B.C.D} {A.B.C.D} creates a static SSM channel table entry by specifying the group and source IP addresses. The first IP address is an IP multicast address within the SSM range. The second IP addres is the source IP adddress and it it is an IP host address that sends traffic to the group.
ssm-map*{A.B.C.D}*[enable]	Enables the administrative state for a specific entry (group). This variable does not affect the dynamically learned entries. This state determines whether the switch uses the static entry or saves it for future use. The default is enable for each entry.

Default

The default IP address for A.B.C.D/X is 232.0.0.0 and the default IP address mask of the multicast group is 255.0.0.0.

The default for {A.B.C.D} {A.B.C.D} enable is enable for each entry.

Command mode

Global Configuration mode

ip igmp (for a VLAN)

Configure Internet Group Management Protocol (IGMP) for each interface to change default multicasting operations.

Syntax

ip igmp compatibility-mode

ip igmp dynamic-downgrade-version

ip igmp last-member-query-interval <0–255> [query-interval <1–65535>] [query-max-response <0–255>] [robust-value <2–255>] [version <1–3>]

ip igmp mrouter {slot/port[-slot/port][,...]}

ip igmp proxy

ip igmp router-alert

ip igmp snooping

ip igmp ssm-snoop

default ip igmp compatibility-mode

default ip igmp dynamic-downgrade-version

default ip igmp last-member-query-interval [query-interval] [query-max-response] [robust-value] [version]

default ip igmp mrouter

default ip igmp proxy

default ip igmp router-alert

default ip igmp snooping

default ip igmp ssm-snoop

no ip igmp compatibility-mode

no ip igmp dynamic-downgrade-version

no ip igmp mrouter {slot/port[-slot/port][,...]}

no ip igmp proxy

no ip igmp router-alert

no ip igmp snooping

no ip igmp ssm-snoop

Parameters

Variable	Value
`compatibility-mode`	Activates v2-v3 compatibility mode. The default value is disabled, which means IGMPv3 is not compatible with IGMPv1 or IGMPv2.
`dynamic-downgrade-version`	Configures if the system downgrades the version of IGMP to handle older query messages. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning.
`last-member-query-interval <0–255>`	Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. Avaya recommends that you configure this value between 3–10 (equal to 0.3 – 1.0 seconds).
`mrouter {slot/port[-slot/port][,...]}`	Adds multicast router ports. {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
`proxy`	Activates the proxy-snoop option globally for the VLAN.
`query-interval <1–65535>`	Configures the frequency (in seconds) at which the VLAN transmits host query packets.
`query-max-response <0–255>`	Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. **Important:** You must configure this value lower than the query-interval.
`robust-value <2–255>`	Configures the expected packet loss of a network. Increase the value if you expect the network to experience packet loss.
`router-alert`	Instructs the router to ignore IGMP packets that do not contain the router alert IP option. When disabled (default configuration), the router processes IGMP

Variable	Value
	packets regardless of the status of the router alert IP option. **Important:** To maximize network performance, Avaya recommends that you configure this parameter according to the version of IGMP currently in use: • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
`snooping`	Activates the snoop option for the VLAN.
`ssm-snoop`	Activates support for PIM-SSM on the snoop interface.
`version <1–3>`	Configures the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version.

Default

The following list provides the default values for command parameters:

- compatibility-mode: disabled
- dynamic-downgrade-version: enabled
- last-member-query-interval: 10 tenths of a second.
- proxy: disabled
- query-interval: 125 seconds.
- query-max-response: 100 tenths of a second (equal to 10 seconds).
- robust-value: 2 seconds
- router-alert: disabled
- snooping: disabled
- ssm-snoop: disabled
- version: 2 (IGMPv2)

Command mode

VLAN Interface Configuration mode

ip igmp (for an Ethernet port)

Configure IGMP for each interface to change default multicasting operations.

Syntax

ip igmp compatibility-mode

ip igmp dynamic-downgrade-version

ip igmp last-member-query-interval <0–255> [query-interval <1–65535>] [query-max-response <0–255>] [robust-value <2–255>] [version <1–3>]

ip igmp router-alert

default ip igmp compatibility-mode

default ip igmp dynamic-downgrade-version

default ip igmp last-member-query-interval [query-interval] [query-max-response] [robust-value] [version]

default ip igmp router-alert

no ip igmp compatibility-mode

no ip igmp dynamic-downgrade-version

no ip igmp router-alert

Parameters

Variable	Value
`compatibility-mode`	Activates v2-v3 compatibility mode. The default value is disabled, which means IGMPv3 is not compatible with IGMPv2.
`dynamic-downgrade-version`	Configures if the system downgrades the version of IGMP to handle older query messages. If the system downgrades, the host with IGMPv3 only capability does not work. If you do not configure the system to downgrade the version of IGMP, the system logs a warning.
`last-member-query-interval <0–255>`	Configures the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages. This value is also the time between group-specific query messages. You cannot configure this value for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. Avaya

Variable	Value
	recommends that you configure this value between 3–10 (equal to 0.3 – 1.0 seconds).
`query-interval <1–65535>`	Configures the frequency (in seconds) at which the VLAN transmits host query packets.
`query-max-response <0–255>`	Configures the maximum response time (in tenths of a second) advertised in IGMPv2 general queries on this interface. You cannot configure this value for IGMPv1. Smaller values allow a router to prune groups faster. **Important:** You must configure this value lower than the query-interval.
`robust-value <2–255>`	Configures the expected packet loss of a network. Increase the value if you expect the network to experience packet loss.
`router-alert`	Instructs the router to ignore IGMP packets that do not contain the router alert IP option. When disabled (default configuration), the router processes IGMP packets regardless of the status of the router alert IP option. **Important:** To maximize network performance, Avaya recommends that you configure this parameter according to the version of IGMP currently in use: • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
`version <1–3>`	Configures the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version.

Default

The following list provides the default values for command parameters:

- compatibility-mode: disabled
- dynamic-downgrade-version: enabled
- last-member-query-interval: 10 tenths of a second.
- query-interval: 125 seconds.
- query-max-response: 100 tenths of a second (equal to 10 seconds).
- robust-value: 2 seconds

- router-alert: disabled
- version: 2 (IGMPv2)

Command mode

GigabitEthernet Interface Configuration mode

ip igmp access-list (for a VLAN)

Configure multicast access control for a VLAN to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

Syntax

ip igmp access-list WORD<1–64> {A.B.C.D/X} <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>

default ip igmp access-list WORD<1–64> {A.B.C.D/X}

no ip igmp access-list WORD<1–64> {A.B.C.D/X}

Parameters

Variable	Value
{A.B.C.D/X}	Creates an access control group entry for a specific IGMP interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1–64>	Specifies the name of the access list from 1–64 characters.

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp access-list (for an Ethernet port)

Configure multicast access control for an IGMP Ethernet port to restrict access to certain multicast streams and to protect multicast streams from spoofing (injecting data to the existing streams).

Syntax

ip igmp access-list WORD<1–64> {A.B.C.D/X} <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both>

default ip igmp access-list WORD<1–64> {A.B.C.D/X}

no ip igmp access-list WORD<1–64> {A.B.C.D/X}

Parameters

Variable	Value
{A.B.C.D/X}	Creates an access control group entry for a specific IGMP interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1–64>	Specifies the name of the access list from 1–64 characters.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

ip igmp access-list mode (for a VLAN)

Change an existing access list on the VLAN interface.

Syntax

ip igmp access-list WORD<1–64> {A.B.C.D/X} mode <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both

default ip igmp access-list WORD<1–64> {A.B.C.D/X}

no ip igmp access-list WORD<1–64> {A.B.C.D/X}

Parameters

Variable	Value
{A.B.C.D/X}	Creates an access control group entry for a specific IGMP interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both	Indicates the action for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
WORD<1–64>	Specifies the name of the access list from 1–64 characters.

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp access-list mode (for an Ethernet port)

Change an existing access list on the Ethernet port.

Syntax

ip igmp access-list WORD<1–64> {A.B.C.D/X} mode <deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both

default ip igmp access-list WORD<1–64> {A.B.C.D/X}

no ip igmp access-list WORD<1–64> {A.B.C.D/X}

Parameters

Variable	Value
`{A.B.C.D/X}`	Creates an access control group entry for a specific IGMP interface. Specify the IP address of the host and the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the network for the host.
`deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both`	Indicates the action for the specified IGMP interface. For example, if you specify deny-both, the interface denies both transmitted and received traffic
`WORD<1–64>`	Specifies the name of the access list from 1–64 characters.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

ip igmp flush port

Use this command to flush Internet Group Management Protocol (IGMP) group members on a port.

Syntax

`ip igmp flush port {slot/port [-slot/port] [,...]} grp-member`

Parameters

Variable	Value
{slot/port [-slot/port] [,...]}	Specifies the port list.
grp-member	Specifies a group member.

Default

None

Command mode

Privileged EXEC mode

ip igmp flush vlan

Use this command to flush Internet Group Management Protocol (IGMP) group members, the multicast router and senders.

Syntax

ip igmp flush vlan <1–4084>

ip igmp flush vlan <1–4084> grp-member

ip igmp flush vlan <1–4084> mrouter

ip igmp flush vlan <1–4084> sender

ip igmp flush vlan <1–4084> sender {A.B.C.D}

ip igmp flush vlan <1–4084>sender {A.B.C.D} {A.B.C.D}

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
grp-member	Specifies a group member.
mrouter	Specifies a multicast router.
sender {A.B.C.D}	Specifies a sender. The first IP address specifies the source IP address of the sender.
sender {A.B.C.D} {A.B.C.D}	Specifies a sender. The first IP address specifies the source IP address of the sender. The second IP address specifies the group IP address of the sender.

Default

None

Command mode

Privileged EXEC mode

ip igmp igmpv3-explicit-host-tracking

Tracks all the source and group members. You must enable explicit-host-tracking to use fast leave for IGMPv3.

Syntax

ip igmp igmpv3-explicit-host-tracking

default ip igmp igmpv3-explicit-host-tracking

no ip igmp igmpv3-explicit-host-tracking

Parameters

None

Default

Disabled

Command mode

Interface Configuration mode

ip igmp immediate-leave (for a VLAN)

Enable fast (immediate) leave mode to specify if a VLAN receives a leave message from a member of a group.

Syntax

ip igmp immediate-leave

default ip igmp immediate-leave

no ip igmp immediate-leave

Parameters

None

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp immediate-leave (for an Ethernet port)

Enable fast (immediate) leave mode to specify if a port receives a leave message from a member of a group.

Syntax

ip igmp immediate-leave

default ip igmp immediate-leave

no ip igmp immediate-leave

Parameters

None

Default

None

Command mode

GigabitEthernet Interface Configuration mode

ip igmp immediate-leave-members

Configure fast leave members on a VLAN to specify fast leave capable ports.

Syntax

ip igmp immediate-leave-members {slot/port[-slot/port][,...]}

default ip igmp immediate-leave-members {slot/port[-slot/port][,...]}

no ip igmp immediate-leave-members {slot/port[-slot/port][,...]}

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp mrdisc

Configure the multicast route discovery options to enable the automatic discovery of multicast-capable routers.

Syntax

ip igmp mrdisc [maxadvertinterval <2–180>] [maxinitadvertinterval <2–180>] [neighdeadinterval <2–180>]

ip igmp mrdisc [maxinitadvertisements <2–15>]

ip igmp mrdisc [minadvertinterval <3–180>]

default ip igmp mrdisc [maxadvertinterval] [maxinitadvertinterval] [neighdeadinterval]

default ip igmp mrdisc [maxinitadvertisements]

default ip igmp mrdisc [minadvertinterval]

no ip igmp mrdisc

Parameters

Variable	Value
maxadvertinterval *<2–180>*	Configures the maximum number (in seconds) between successive advertisements. For this change to take effect, you must save the configuration, and then reset the switch.
maxinitadvertinterval <2–180>	Configures the maximum number (in seconds) between successive initial advertisements. For this change to take effect, you must save the configuration, and then reset the switch.
maxinitadvertisements <2–15>	Configures the maximum number of initial multicast advertisements after initialization. For this change to take effect, you must save the configuration, and then reset the switch.
minadvertinterval *<3–180>*	Configures the minimum number (in seconds) between successive advertisements. For this change to take effect, you must save the configuration, and then reset the switch.
neighdeadinterval *<2–180>*	Configures the multicast router discovery dead interval—the number of seconds the multicast route neighbors for the switch must wait before assuming that the multicast router is down.

Default

The following list provides the default values for command parameters:

- maxadvertinterval: 20
- maxinitadvertinterval : 2
- maxinitadvertisements: 3

- minadvertinterval: 15
- neighdeadinterval: 60

Command mode

VLAN Interface Configuration mode

ip igmp static-group

Configure IGMP static members to add members to a snoop group.

Syntax

`ip igmp static-group {A.B.C.D} {A.B.C.D} {port [slot/port[-slot/port][,...]]} [static|blocked]`

Parameters

Variable	Value
[static|blocked]	Adds a static-member entry to the IGMP interface. • *value* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • **`static|blocked`** configures the route to static or blocked.
{slot/port [-slot/port][,...]}	Creates static members on the interface. Specifies the port or list of ports to which you want to redirect the multicast stream for this multicast group. Use the format {slot/port[-slot/port][,...]}. Use the **no** operator to later remove this configuration.
<*A.B.C.D*> <*A.B.C.D*>	Indicates the IP address range from <*A.B.C.D*> to <*A.B.C.D*>of the selected multicast group.

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp stream-limit (for an Ethernet port)

Configure multicast stream limitation on an Ethernet port to limit the number of concurrent multicast streams on the port.

Syntax

ip igmp stream-limit [stream-limit-max-streams <0–65535>]

Parameters

Variable	Value
stream-limit	Enables the stream limit on the specifies Ethernet port.
stream-limit-max-streams <*0–65535*>	Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

ip igmp stream-limit-group

Configure multicast stream limitation members on ports of a specific VLAN to limit the number of multicast groups that can join a VLAN.

Syntax

ip igmp stream-limit-group {slot/port [-slot/port][,...]} enable max-streams <0–65535>

Parameters

Variable	Value
max-streams <*0–65535*>	Configures the maximum number of allowed streams for the specified ports on this VLAN. The range is from 0–65535 and the default is 4.

Variable	Value
	To use the default configuration, use the default option in the command: **default ip igmp stream-limit-group <ports>**
{slot/port [-slot/port][,...]}	Specifies the slot and the port number.

Default

None

Command mode

VLAN Interface Configuration mode

ip igmp stream-limit (for a VLAN)

Configure multicast stream limitation on a VLAN to limit the number of concurrent multicast streams on the VLAN.

Syntax

ip igmp stream-limit [stream-limit-max-streams <0–65535>]

Parameters

Variable	Value
stream-limit	Enables the stream limit on the specifies VLAN port.
stream-limit-max-streams <*0–65535*>	Sets the maximum number of streams allowed on an interface. The value ranges from 0 to 65535.

Default

None

Command mode

VLAN Interface Configuration mode

ip mroute resource-usage egress-threshold

Configure the resource usage counters to query the number of ingress and egress IP multicast streams traversing your switch.

Syntax

ip mroute resource-usage egress-threshold <0–32767> ingress-threshold <0–32767>

Parameters

Variable	Value
egress-threshold *<0–32767>*	Configures the egress record threshold (S,G). A notification message is sent if this value is exceeded. • *integer* is a value between 0–32767. To set this option to the default value, use the **default** operator with the command. The default is 0.
ingress-threshold *<0–32767>*	Configures the ingress record threshold (peps). A notification message is sent if this value is exceeded. • *integer* is a value between 0–32767. To set this option to the default value, use the **default** operator with the command. The default is 0.

Default

None

Command mode

Global Configuration mode

ip mroute resource-usage log-msg trap-msg

Enable traps and log messages on the console.

Syntax

ip mroute resource-usage log-msg trap-msg

Parameters

Variable	Value
log-msg	Configures the notification method for sending only a log message after the threshold level is exceeded. Use the **no**

Variable	Value
	operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is disabled.
trap-msg	Configures the notification method for sending only a trap message after the threshold level is exceeded. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is disabled.

Default

None

Command mode

Global Configuration mode

ip mroute static-source-group

Configure static source-group entries in the Protocol Independent Multicast (PIM) multicast routing table.

Syntax

ip mroute static-source-group <A.B.C.D> <A.B.C.D/X>

Parameters

Variable	Value
A.B.C.D	Specifies the IP address of the multicast group. Use the **no** operator to remove this configuration.
A.B.C.D/X	Specifies the multicast source IP address and subnet mask for the static source group entry. You cannot create duplicate groups. How you configure the source address depends on the protocol and mode you use. Use the **no** operator to remove this configuration.

Default

None

Command mode

Global Configuration mode

ip mroute stream-limit (globally)

Limit the number of multicast streams to protect a Central Processor Unit (CPU) from multicast data packet bursts generated by malicious applications.

Syntax

`ip mroute stream-limit`

Parameters

None

Default

None

Command mode

Global Configuration mode

ip mroute stream-limit (for a port)

Limit the number of multicast streams to protect a CPU from multicast data packet bursts generated by malicious applications.

Syntax

`ip mroute stream-limit`

Parameters

Variable	Value
max-allowed-streams *<1-32768>*	Configures the maximum number of streams on the specified port. The port is shut down if the number of streams exceeds this limit. The value is a number between 1–32768. The default value is 1984 streams. To set this option to the default value, use the **`default`** operator with the command.
max-allowed-streams-timer-check *<1–3600>*	Configures the sampling interval, which is used to check if the number of ingress multicast streams to the CPU is under a configured limit or if the port needs to shut down. The range is between 1–3600. The default value is 10 seconds. To set this option to the default value, use the **`default`** operator with the command.

Variable	Value
port *{slot/port [-slot/port][,...]}*	Specifies the port or range of ports in slot/port notation. Use the **no** operator to later remove this configuration.
stream-limit	Enables stream limit on a particular interface.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

ip pim bsr-candidate preference

Configure additional routers as candidate BSRs (C-BSR) to provide backup protection in the event that the primary BSR fails.

Syntax

ip pim bsr-candidate preference <0–255>

no ip pim bsr-candidate

default ip pim bsr-candidate

Parameters

Variable	Value
preference *<0–255>*	Enables the C-BSR on this interface and configures its preference value, from 0–255, to become a BSR. The C-BSR with the highest BSR preference and address is the preferred BSR.

Default

None

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ip pim active

Enable PIM and configure the interface type to active or passive to perform multicasting operations.

Syntax

`ip pim <active|passive>`

Parameters

Variable	Value
active	Enables PIM and sets interface type to active.
passive	Enables PIM and sets interface type to passive.

Default

None

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ip pim enable (globally)

Configure PIM-SM to enable or disable PIM-SM globally on the switch and change default global parameters.

Syntax

`ip pim enable`

`default ip pim enable`

Parameters

Variable	Value
enable	Globally activates PIM on the switch.

Default

The default is disabled.

Command mode

Global Configuration mode

Related commands

Variable	Value
bootstrap-period <*5–32757*>	Specifies the interval (in seconds) that the elected bootstrap router (BSR) waits between originating bootstrap messages. • <*5–32757*> is an integer in the range of 5–32757. The default is 60. To set this option to the default value, use the **default** operator with the command.
disc-data-timeout <*5–65535*>	Specifies how long (in seconds) to discard data until the join is received from the rendezvous point (RP). An IP multicast discard record is created after a register packet is sent, until the the timer expires or a join is received. • <*5–65535*> is an integer in the range of 5–65535. The default is 60. To set this option to the default value, use the **default** operator with the command.
fast-joinprune	Enables the fast join prune interval. To set this option to the default value, use the **default** operator with the command. The default is disabled.
fwd-cache-timeout <*10–86400*>	Specifies the forward cache timeout value. • <*10–86400*> is an integer in the range of 10–86400. The default is 210. To set this option to the default value, use the **default** operator with the command.
join-prune-interval <*1–18724*>	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. • <*1–18724*> is an integer in the range of 1–18724. The default is 60. To set this option to the default value, use the **default** operator with the command.
mode <*sparse*|*ssm*>	Configures the mode of this interface globally. After you change from one mode to another, an information message appears to remind you that traffic does not stop immediately. To set this option to the default value, use the **default** operator with the command. The default is sparse.
register-suppression-timeout <*6–65535*>	Specifies how long (in seconds) the designated router (DR) suppresses sending registers to the RP. The timer starts

Variable	Value
	after the DR receives a register-stop message from the RP. • *<6–65535>* is an integer in the range of 6–65535. The default is 60. To set this option to the default value, use the **default** operator with the command.
rp-c-adv-timeout *<5–26214>*	Specifies how often (in seconds) a router configured as a candidate RP (C-RP) sends C-RP advertisement messages. After this timer expires, the C-RP router sends an advertisement message to the elected BSR. • *<5–26214>* is an integer in the range of 5–26214. The default is 60. To set this option to the default value, use the **default** operator with the command.
rp-candidate group *<A.B.C.D>* *<mask address>* rp *<A.B.C.D>*	Adds or deletes candidate RP entries. Use the **no** operator to later remove this configuration.
static-rp *<A.B.C.D/X>* *<A.B.C.D>*	Adds static RP entries and activates static RP. A.B.C.D/X represents the group address and mask. A.B.C.D is the RP IP address.
unicast-route-change-timeout *<2–65535>*	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates for PIM. **Important:** Lowering this value increases how often the switch polls the RTM. This can affect the performance of the switch, especially when a high volume of traffic flows through the switch. • *<2–65535>* is an integer in the range of 2–65535. The default is 5. To set this option to the default value, use the **default** operator with the command.
virtual-neighbor *<A.B.C.D>* *<A.B.C.D>*	Adds a virtual neighbor to an interface globally. A.B.C.D represents the IP addresses of the interface and the virtual neighbor. Use the **no** operator to later remove this configuration.

ip pim enable (for an Ethernet port or VLAN)

Configure PIM for each interface to enable the interface to perform multicasting operations.

Syntax

ip pim enable

default ip pim enable

no ip pim enable

Parameters

Variable	Value
enable	Enables PIM on the local switch interface. To set this option to the default value, use the default operator with the command. The default is disabled.

Default

Disabled

Command mode

VLAN and GigabitEthernet Interface Configuration mode

Related commands

Variable	Value
active	Enables PIM and configures the interface type to active.
bsr-candidate preference *<0-255>*	Enables the BSR candidate on a specific port. The preference value ranges from 0–255. Use the no operator to later remove this configuration. To set this option to the default value, use the default operator with the command. The default is disabled.
hello-interval *<0-18724>*	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds with the range of 0–18724. To set this option to the default value, use the default operator with the command.
interface-type <active| passive>	Specifies whether the selected interface is active or passive. You can change the state of a PIM interface after you create the interface but only if you disable PIM on the interface. An active interface accepts PIM control transmitted and received traffic. A passive interface prevents PIM control traffic from transmitting or receiving, thereby reducing the load on a system. This feature is useful when a high number of PIM interfaces exist and connect to end users, not to other switches. To set this option to the default value, use the default operator with the command. The default is active.
joinprune-interval *<1-18724>*	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default is 60 seconds. To set this option to the

Variable	Value
	default value, use the default operator with the command. The range is 1–18724.
passive	Enables PIM and configures the interface type to passive.

ip pim mode ssm

Configure SSM to optimize PIM-SM by simplifying the many-to-many model (servers-to-receivers).

Syntax

`ip pim mode <ssm|sparse>`

Parameters

None

Default

None

Command mode

Global Configuration mode

ip pim rp-candidate group

Configure a candidate rendezvous point (C-RP) to serve as backup to the RP router.

Syntax

`ip pim rp-candidate group <A.B.C.D> <A.B.C.D> rp <A.B.C.D>`

Parameters

Variable	Value
group *<A.B.C.D>*	Specifies the IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
<A.B.C.D>	Specifies the address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP router.
rp *<A.B.C.D>*	Specifies the IP address of the C-RP router. This address must be one of the local PIM-SM enabled interfaces.

Default

None

Command mode

Global Configuration mode

ip pim static-rp

Configure a static RP to configure a static entry for an RP.

Syntax

ip pim static-rp <A.B.C.D/X> <A.B.C.D>

Parameters

Variable	Value
<A.B.C.D/X>	Specifies the IP address and address mask of the multicast group. When combined, the IP address and address mask identify the range of the multicast addresses that the RP handles.
<A.B.C.D>	Specifies the IP address of the static RP.

Default

None

Command mode

Global Configuration mode

ip pim virtual-neighbor

Configure a virtual neighbor when the next hop for a static route cannot run PIM.

Syntax

ip pim virtual-neighbor <A.B.C.D> <A.B.C.D>

Parameters

Variable	Value
<A.B.C.D>	The first IP address indicates the IP address of the selected interface.

Variable	Value
<A.B.C.D>	The second IP address Indicates the IP address of the neighbor.

Default

None

Command mode

Global Configuration mode

multicast smlt-square

Enable square-SMLT globally on each of the four switches to form an SMLT aggregation group.

Syntax

`multicast smlt-square`

Parameters

Variable	Value
smlt-square	Enables multicast SMLT square.

Default

None

Command mode

Global Configuration mode

multicast software-forwarding

Configure the IP multicast software forwarding feature so the CPU initially forwards IP multicast data until a hardware record is created.

Syntax

`multicast software-forwarding`

Parameters

None

Default

None

Command mode

Global Configuration mode

route-map policy name seq number

Create and configure the policy before you apply and announce or accept policy to an interface, VLAN, or a port.

Syntax

`route-map WORD<1–64> <1–65535>`

Parameters

Variable	Value
WORD<1–64>	Indicates the name of the specified policy with a string length of 1 to 64 characters.
<1–65535>	Indicates the number of the specified policy in the range of 1 to 65535.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
enable	Enables a route policy with a policy name and a sequence number. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **`default`** operator with the command. The default is disabled.
match as-path *WORD<0–256>*	If configured, the switch matches the as-path attribute of the Border Gateway Protocol (BGP) routes against the contents of the specified as-lists. This field is used

Variable	Value
	only for BGP routes and ignored for all other route types. • *as-list* specifies the list IDs of up to four as-lists, separated by commas. Use the **no** operator to later remove this configuration.
match community *WORD <0–256>*	If configured, the switch matches the community attribute of the BGP routes against the contents of the specified community-lists. This field is used only for BGP routes and ignored for all other route types. • *community-list* specifies the list IDs of up to four defined community-lists, separated by commas. Use the **no** operator to later remove this configuration.
match community-exact enable	When disabled, match-community results in a match when the community attribute of the BGP routes matches an entry of a community-list specified in match-community. When enabled, match-community results in a match when the community attribute of the BGP routes matches all of the entries of all the community-lists specified in match-community. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is disabled.
match extcommunity*WORD<0–1027>*	Matches the community in the community-id list where **word** is between 0–1027. Represent multiple community-id list as 2,4,5,6,7.
match interface *WORD<0–259>*	If configured, the switch matches the IP address of the interface from which the RIP route was learned against the contents of the specified prefix list. This field is used only for RIP routes and ignored for all other route types. • *prefix-list* specifies the names of up to four defined prefix lists, separated by commas. Use the **no** operator to later remove this configuration.
match local-preference *<0-2147483647>*	Matches the preference value from 0–2147483647. To set this option to the default value, use the **default** operator with the command. The default is 0.

Variable	Value
match metric *<0-65535*	If configured, the switch matches the metric of the incoming advertisement or existing route against the specified value. If 0, this field is ignored. • *metric* is 0–65535. The default is 0. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command.
match network *WORD<0–259>*	If configured, the switch matches the destination network against the contents of the specified prefix lists. • *prefix-list* specifies the names of up to four defined prefix lists, separated by commas. Use the **no** operator to later remove this configuration.
match next-hop*WORD<0–259>*	If configured, matches the next-hop IP address of the route against the contents of the specified prefix list. This field applies only to nonlocal routes. • *prefix-list* specifies the names of up to four defined prefix lists, separated by commas. Use the **no** operator to later remove this configuration.
match protocol*Any|xxx WORD<0–40>*	If configured, matches route policy to the protocol from which the route is learned. xxx is local, ospf, ebgp, ibgp, rip, static, or a combination separated by a vertical bar (|). This field is used only for Routing Information Protocol (RIP) announcement purposes. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is any.
match route-source *WORD<0–259>*	If configured, matches the next-hop IP address for RIP and BGP routes and advertising router IDs for Open Shortest Path First (OSPF) routes against the contents of the specified prefix list. This option is ignored for all other route types. • *prefix-list* specifies the names of up to four defined prefix lists, separated by commas. Use the **no** operator to later remove this configuration.
match route-type *<any|local|internal|external|external-1|external-2>*	Configures a specific route-type to match (applies only to OSPF routes).

Variable	Value
	Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is any.
match tag *WORD<0–256>*	Specifies a list of tags that is used during the match criteria process. Contains one or more tag values. • *tag* is a value from 0–256. Use the **no** operator to later remove this configuration.
vrf*WORD<0–16>*	Match the VRF name.
vrfids*WORD<0–511>*	Match a range of VRFs.
name *WORD<1–64>*	Renames a policy after its creation. This command changes the name field for all sequence numbers under the policy.
<permit|deny>	Specifies the action to take when a policy matches a specific route. Permit accepts the route and deny ignores the route. To set this option to the default value, use the **default** operator with the command. The default is permit.
<0–65535>	Indicates the number of the specified policy, which is a number from 1–65535.
set as-path *WORD<0–256>*	If configured, the switch adds the as-number of the as-list to the BGP routes that match this policy. • *as-list-id* specifies the list ID of up to four defined as-lists, separated by commas. Use the **no** operator to later remove this configuration.
set as-path-mode <tag|prepend>	**prepend** is the default configuration. The switch prepends the as-number of the as-list specified in set-as-path to the old as-path attribute of the BGP routes that match this policy. Use the **no** operator to later remove this configuration.
set automatic-tag <enable>	Configures the tag automatically. This option is used for BGP routes only. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is disabled.

Variable	Value
set community *WORD<0–256>*	If configured, the switch adds the community number of the community list to the BGP routes that match this policy. • *community-list* specifies the list ID of up to four defined community lists, separated by commas. Use the **no** operator to later remove this configuration.
set community-mode <additive|none|unchanged>	Configures the community mode. • **additive**—the switch prepends the community number of the community list specified in set-community to the old community path attribute of the BGP routes that match this policy. • **none**—the switch removes the community path attribute of the BGP routes that match this policy. • **unchanged**—keeps the community attribute in the route path. Use the **no** operator to later remove this configuration. The default is unchanged.
set injectlist *WORD<0–1027>*	If configured, the switch replaces the destination network of the route that matches this policy with contents of the specified prefix list. • *prefix-list* specifies one prefix list by name. Use the **no** operator to later remove this configuration.
set local-preference *<0-65535>*	A value used during a route decision process in the BGP protocol. Applicable to BGP only. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.
set mask *<A.B.C.D>*	If configured, the switch configures the mask of the route that matches this policy. This applies only to RIP accept policies. • *ipaddr* is a valid contiguous IP mask. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.0.0.0.
set metric *<0-65535>*	If configured, the switch configures the metric value for the route while announcing a redistribution. The default is 0. If the default is configured, the original cost

Variable	Value
	of the route is advertised into OSPF; for RIP, the original cost of the route or default-import-metric is used. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command.
set metric-type <*type1*|*type2*>	If configured, sets the metric type for the routes that match this policy to announce into the OSPF domain. The default is type 2. This variable is applicable only for OSPF announce policies. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command.
set metric-type-internal	Sets the internal metric type, 0 or 1. To set this option to the default value, use the **default** operator with the command. The default is 0.
set next-hop <*A.B.C.D*>	Specifies the IP address of the next-hop router.Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.0.0.0.
set nssa-pbit enable	Configures the not-so-stubby-area (NSSA) translation P bit. This variable is applicable only for OSPF announce policies. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is enable.
set origin <*igp*|*egp*|*incomplete*>	If configured, the switch changes the origin path attribute of the BGP routes that match this policy to the specified value. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is unchanged (not configured).
set origin-egp-as <*0-65535*>	Indicates the remote autonomous system number. This variable is applicable to BGP only. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.
set tag <*0-65535*>	Configures the tag of the destination routing protocol. If you do not specify a tag, the switch forwards the tag value in the source routing protocol. A value of zero indicates that this parameter is not set. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.

Variable	Value
set weight <*0-65535*>	The weight value for the routing table. For BGP, this value overrides the weight configured through NetworkTableEntry, FilterListWeight, or NeighborWeight. This parameter is applicable to BGP only. A value of zero indicates that this parameter is not set. Use the **no** operator to later remove this configuration. To set this option to the default value, use the **default** operator with the command. The default is 0.

show debug

Shows Protocol Independent Multicast (PIM) debug configuration.

Syntax

show debug ip pim

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip arp static-mcastmac

Display Layer 3 multicast MAC ARP data.

Syntax

show ip arp static-mcastmac [-s <A.B.C.D/X> [vrf WORD<0–16>] [vrfids WORD<0–512>] [<A.B.C.D>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp access

Display information about the Internet Group Management Protocol (IGMP) multicast access control groups.

Syntax

show ip igmp access

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp cache

Display information about the IGMP cache.

Syntax

show ip igmp cache

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp group

Display information about a statically configured or dynamically learned IGMP group.

Syntax

show ip igmp group [count]

show ip igmp group group <A.B.C.D> [detail] [vlan <1–4084>] [port {slot/port[-slot/port][,...]}]

show ip igmp group group <A.B.C.D> [tracked-members] [vlan <1–4084>] [port {slot/port[-slot/port][,...]}] [source-subnet <A.B.C.D/X>] {member-subnet <A.B.C.D./X>]

Parameters

Variable	value
count	Displays the number of entries in the IGMP group
detail	Use the detail parameter to show IGMPv3–specific data.
group *<A.B.C.D>*	Specifies the address of the IGMP group.
member-subnet {default| *<A.B.C.D>*}]	Specifies the IP address and mask of the IGMP member.
port *{slot/port[-slot/port][,...]}*	Specifies the port list.
source-subnet *<A.B.C.D/X>*	Specifies the source IP address and the subnet mask.
tracked-members	Use the tracked-members parameter to view all the tracked members for a specific group.
vlan *<1–4084>*	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show ip igmp interface

Display information about the interfaces where Internet Group Management Protocol (IGMP) is enabled.

Syntax

show ip igmp interface gigabitethernet [{slot/port[-slot/port][,...]}] [<1–4084>]

show ip igmp interface vlan [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
gigabitethernet *{slot/port[-slot/port][,...]}*	Specifies the port.
interface	Shows IGMP interfaces.
vlan *<1–4084>*	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show ip igmp mrdisc

Display information about the IGMP multicast discovery routes.

Syntax

`show ip igmp mrdisc`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp mrdisc neighbors

Display information about the IGMP multicast router discovery neighbors.

Syntax

`show ip igmp mrdisc neighbors`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp router-alert

Display the status of IGMP router alert.

Syntax

show ip igmp router-alert

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp sender

Display information about the IGMP senders.

Syntax

show ip igmp sender [count] [group <A.B.C.D>] [member-subnet <A.B.C.D/mask>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp snooping

Display the status of IGMP snoop.

Syntax

show ip igmp snooping

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp snoop-trace

View multicast group trace information for IGMP snoop.

Syntax

show ip igmp snoop-trace [source <A.B.C.D>] [group <A.B.C.D>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp ssm

Display the SSM group range and the status of dynamic learning.

Syntax

show ip igmp ssm

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp ssm-map

Display the list of SSM channels.

Syntax

show ip igmp ssm-map

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp static

Display information about the static and blocked ports for the IGMP-enabled interfaces.

Syntax

show ip igmp static

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip igmp stream-limit interface

Display multicast stream limitation information for the ports on a specific interface.

Syntax

`show ip igmp stream-limit <interface|port>`

Parameters

Variable	Value
Interface	Specifies the type of interface to include in the output. The results display all ports using stream limitation on the selected interface type.
port	Specifies the IGMP stream limitation port details.

Default

None

Command mode

Privileged EXEC mode

show ip igmp sys

View the current fast leave mode configuration and IGMP system parameters on the switch.

Syntax

`show ip igmp sys`

Parameters

None

Default

None

Command mode

Global Configuration mode

show ip mroute hw-resource-usage

View multicast hardware resource usage.

Syntax

show ip mroute hw-resource-usage

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip mroute interface

Display information about the multicast routes set up on the switch for a specific interface.

Syntax

show ip mroute interface gigabitethernet {slot/port[-slot/port] [,....]}

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip mroute next-hop

Display information about the next hop for the multicast routes set up on the switch.

Syntax

show ip mroute next-hop

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip mroute route

Display information about the multicast routes set up on the switch.

Syntax

show ip mroute route

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip mroute static-source-group

Display information about the static source groups on the current interface.

Syntax

show ip mroute static-source-group <A.B.C.D>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim

Verify the configuration by displaying the global status of PIM on the switch.

Syntax

show ip pim

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim active-rp

Display information about the active rendezvous point (RP) for all groups or a specific group.

Syntax

show ip pim active-rp group <A.B.C.D>

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim bsr

Display information about the bootstrap router (BSR) for this PIM-SM domain.

Syntax

show ip pim bsr

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim interface

Display information about the PIM-SM interface setup on the switch.

Syntax

show ip pim interface [gigabitethernet [{slot/port [-slot/port] [,...]}] [<1–4084>]

show ip pim interface vlan [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
gigabitethernet *{slot/port [-slot/port][,...]}*	Displays configuration settings for the gigabitethernet interface.
vlan *[<1–4084>]*	Displays configuration setting for a VLAN interface.

Default

None

Command mode

Privileged EXEC mode

show ip pim mode

Show the PIM mode (SM or SSM) configuration on the switch.

Syntax

show ip pim mode

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim mroute

Display information from the route table.

Syntax

show ip pim mroute [source <A.B.C.D>] [group <A.B.C.D>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim neighbor

Display information about the neighboring routers configured with PIM-SM.

Syntax

show ip pim neighbor

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim rp-candidate

Display information about the candidate rendezvous points for the PIM-SM domain.

Syntax

show ip pim rp-candidate

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim rp-hash

Display information about the RPs for this PIM-SM domain.

Syntax

show ip pim rp-hash

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim static-rp

Display the static RP table.

Syntax

show ip pim static-rp

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip pim virtual-neighbor

Display the virtual neighbor.

Syntax

show ip pim virtual-neighbor

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show multicast software-forwarding

Show the software forwarding configuration.

Syntax

show multicast software-forwarding

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show multicast square-smlt

Show the multicast square MLT distribution configuration.

Syntax

`show multicast square-smlt`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show vlan static-mcastmac

Display the Layer 2 multicast media access control (MAC) filters.

Syntax

`show vlan static-mcastmac [<1–4084>]`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

Chapter 10: IPv6 routing commands

This chapter provides the Avaya Command Line Interface (ACLI) commands to perform general IPv6 routing operations on the Avaya Virtual Services Platform 9000.

clear ipv6 dcache

Clear the destination cache.

Syntax

clear ipv6 dcache [gigabitethernet <slot/port>] [mgmtethernet <slot/port>] [tunnel <1–2000>] [vlan <1–4084>]

Parameters

Variable	Value
gigabitethernet <*slot/port*>	Specifies the slot and port.
mgmtethernet <*slot/port*>	Specifies the slot and port. To identify a management port use 1/1 or 2/1.
tunnel <*1–2000*>	Specifies a tunnel ID.
vlan <*1–4084*>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

clear ipv6 neighbor-cache

Clear the neighbor cache.

Syntax

clear ipv6 neighbor-cache

clear ipv6 neighbor-cache gigabitEthernet <slot/port>

clear ipv6 neighbor-cache mgmtethernet <slot/port>

clear ipv6 neighbor-cache vlan <1–4084>

Parameters

Variable	Value
neighbor-cache	Clears the neighbor cache for an interface.
gigabitethernet <*slot/port*>	Specifies the slot and port.
mgmtethernet <*slot/port*>	Specifies the slot and port. To identify a management port use 1/1 or 2/1.
vlan <*1–4084*>	Specifies the VLAN ID.

Default

The default is disabled.

Command mode

Privileged EXEC mode

clear ipv6 route static

Clear IPv6 static routes.

Syntax

clear ipv6 route static

Parameters

None

Default

None

Command mode

Privileged EXEC mode

ipv6 area

Create and configure an OSPFv3 IPv6 area.

Syntax

ipv6 area {A.B.C.D} [default-cost <0–16777215>] [translator-role {1|2}]

ipv6 area {A.B.C.D} [import-summaries enable]

ipv6 area {A.B.C.D} [import <external|noexternal|nssa>]

ipv6 area {A.B.C.D} [type {nssa|stub}] [default-cost <0–16777215>] [translator-role {1|2}]

default ipv6 area {A.B.C.D} [default-cost]

default ipv6 area {A.B.C.D} [import-summaries enable]

default ipv6 area {A.B.C.D} [import]

no ipv6 area {A.B.C.D} [import-summaries enable]

Parameters

Variable	Value
{A.B.C.D}	Specifies the area address.
default-cost *<0–16777215>*	Specifies the stub metric for the area.
import <*external*|*noexternal*|*nssa*>	Configures the area support for importing advertisements.
import-summaries enable	Configures the area support for importing summary advertisements into a stub area. Use this entry only for a stub area.
translator-role *{1|2}*	Indicates an NSSA border router ability to perform translation of type-7 LSAs into type-5 LSAs. Configure this value to 2 to make it a candidate. You can configure this parameter only when you first create the area.
type *{nssa|stub}*	Configures the type of area. An NSSA prevents flooding of normal route advertisements into the area by replacing them with a default route. A stub area uses only one exit point (router interface) out of the area. You can configure this parameter only when you first create the area.

Default

The default cost is 10. The default import is external. The default to import-summaries is enabled. The default translator role is 1. By default, the area is neither a stub area or an NSSA.

Command mode

OSPF Router Configuration mode

ipv6 area range

Create and configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas.

Syntax

ipv6 area range {A.B.C.D} WORD<0–255> advertise-mode <advertise|not-advertise>

ipv6 area range {A.B.C.D} WORD<0–255> <inter-area-prefix-link|nssa-extlink> advertise-mode <advertise|not-advertise> [advertise-metric <0–65535>]

default ipv6 area range {A.B.C.D} WORD<0–255> inter-area-prefix-link [advertise-metric]

default ipv6 area range {A.B.C.D} WORD<0–255> nssa-extlink [advertise-metric]

no ipv6 area range {A.B.C.D} WORD<0–255> inter-area-prefix-link

no ipv6 area range {A.B.C.D} WORD<0–255> nssa-extlink

Parameters

Variable	Value
{A.B.C.D}	Specifies the area address.
advertise-metric *<0–65535>*	Specifies the advertise metric value and LSA type.
advertise-mode *<advertise|not-advertise>*	Configures if the area advertises into other OSPF areas.
inter-area-prefix-link	Configures the area to use this LSA type.
nssa-extlink	Configures the area to use this LSA type.
WORD<0–255>	Specifies the IPv6 address and prefix.

Default

The default advertise metric is 0. The default advertise-mode is advertise.

Command mode

OSPF Router Configuration mode

ipv6 area virtual-link

Configure an OSPF virtual interface to the ABR if a remote OSPF ABR uses no connection to the backbone area but needs to be part of the same routing domain in which the switch resides.

Syntax

ipv6 area virtual-link {A.B.C.D} {A.B.C.D} [dead-interval <1–65535>] [retransmit-interval <1–1800>] [transit-delay <1–1800>]

ipv6 area virtual-link {A.B.C.D} {A.B.C.D} [hello-interval <1–65535>] [dead-interval <1–65535>] [retransmit-interval <1–1800>] [transit-delay <1–1800>]

default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} [dead-interval] [retransmit-interval] [transit-delay]

default ipv6 area virtual-link {A.B.C.D} {A.B.C.D} [hello-interval] [dead-interval] [retransmit-interval] [transit-delay]

no ipv6 area virtual-link {A.B.C.D} {A.B.C.D}

Parameters

Variable	Value
{A.B.C.D} {A.B.C.D}	Specifies the area address and the virtual link address.
dead-interval *<1–65535>*	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down.
hello-interval *<1–65535>*	Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area.
retransmit-interval *<1–1800>*	Specifies the retransmit interval, in seconds, for link-state advertisements.
transit-delay *<1–1800>*	Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface.

Default

The default dead interval is 60. The default hello interval is 10. The default retransmit interval is 5. The default transit-delay is 1.

Command mode

OSPF Router Configuration mode

ipv6 as-boundary-router

Enables or disables the boundary-router on the router interface.

Syntax

ipv6 as-boundary-router [enable]

default ipv6 as-boundary-router [enable]

no ipv6 as-boundary-router [enable]

Parameters

Variable	Value
enable	Enables the boundary-router.

Default

The default is disabled.

Command mode

OSPF Router Configuration mode

ipv6 dhcp-relay (on an interface)

Configures DHCP Relay on an interface.

Syntax

ipv6 dhcp-relay [max-hop <1-32>]

ipv6 dhcp-relay [remoteId]

ipv6 dhcp-relay fwd-path WORD<0-255> [vrid WORD<1-255>] [enable]

default ipv6 dhcp-relay [max-hop] [remoteId]

default ipv6 dhcp-relay fwd-path WORD<0-255>

no ipv6 dhcp-relay [remoteId]

Note:

The command **no ipv6 dhcp-relay** disables DHCP on the interface, it does not delete the entry.

no ipv6 dhcp-relay fwd-path WORD<0-255> [enable]

Parameters

Variable	Value
max-hop <*1-32*>	Configures the maximum number of hops before a BootP/DHCP packet is discarded.
remoteId	Enables the Remote ID.
vrid *WORD<1-255>*	Specifies the ID of the virtual router and is an integer from 1–255.
WORD<0-255>	Creates a forwarding path to the DHCP server with a mode and a state. WORD<0-255> is the IPv6 address of the server. The default IP address of the relay is the address of the interface. **Tip:** If the relay is a Virtual Router configured on this interface, you must set the vrid.

Default

The default max hop is 32. The remote ID is disabled by default. The forwarding path is disabled by default.

Command mode

Interface Configuration mode

ipv6 dhcp-relay fwd-path

Create the forwarding path from the client to the server.

Syntax

ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> [enable]

default ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> [enable]

no ipv6 dhcp-relay fwd-path WORD<0-255> WORD<0-255> [enable]

Parameters

Variable	Value
enable	Enables the forwarding path to the server.
WORD<0-255> WORD<0-255>	Configures the forwarding path from the client to the server. • The first **WORD<0-255>** is the IP address configured on an interface (a locally configured IP address) to forward or relay BootP or DHCP. This address is the relay agent. The relay can be a VRRP address. • The second **WORD<0-255>** is the IP address of the DHCP server in the network. If this IP address corresponds to the locally configured IP network the system generates an error because IPv6 does not include broadcast..

Default

The default is disabled.

Command mode

Global Configuration mode

ipv6 forwarding

Configures IPv6 forwarding. By default, IPv6 forwarding is globally disabled, which means you can only use local IPv6 connections, and traffic does not traverse an IPv6 network.

Syntax

ipv6 forwarding

default ipv6 forwarding

no ipv6 forwarding

Parameters

None

Default

By default forwarding is globally disabled but enabled on an interface. You must enable it globally before the interface configuration takes effect.

Command mode

Global Configuration mode, GigabitEthernet Interface Configuration mode, and VLAN Interface Configuration mode

ipv6 hop-limit

Inserts a value into the hop-limit field of the IPv6 header.

Syntax

ipv6 hop-limit <0-255>

default ipv6 hop-limit <0-255>

Parameters

Variable	Value
<0–255>	Inserts a value into the hop-limit field of IPv6 header in the range of 0 to 255.

Default

The default hop limit is 64.

Command mode

Global Configuration mode

ipv6 icmp error-interval

Configures the interval (in milliseconds) for sending ICMPv6 error messages.

Syntax

ipv6 icmp error-interval <0-2147483647>

default ipv6 icmp error-interval

Parameters

Variable	Value
<0–2147483647>	Configures the interval (in milliseconds) for sending ICMPv6 error messages. An entry of

Variable	Value
	0 seconds results in no sent ICMPv6 error messages

Default

The default error interval is 1000.

Command mode

Global Configuration mode

ipv6 icmp error-quota

Configures the number of ICMP error messages that can be sent during the ICMP error interval.

Syntax

ipv6 icmp error-quota <0-2000000>

default ipv6 icmp error-quota

Parameters

Variable	Value
<0-2000000>	Configures the number of ICMP error messages that the system can send during the ICMP error interval. A value of zero instructs the system not to send any ICMP error messages.

Default

The default error quota is 50.

Command mode

Global Configuration mode

ipv6 icmp redirect-msg

Enables ICMP redirect messages.

Syntax

ipv6 icmp redirect-msg

default ipv6 icmp redirect-msg

no ipv6 icmp redirect-msg

Parameters

None

Default

By default ICMP redirect messages are disabled.

Command mode

Global Configuration mode

ipv6 icmp unreach-msg

Enables ICMP network unreachable messages.

Syntax

ipv6 icmp unreach-msg

default ipv6 icmp unreach-msg

no ipv6 icmp unreach-msg

Parameters

None

Default

By default ICMP network unreachable messages are disabled.

Command mode

Global Configuration mode

ipv6 interface address (for a port)

Configure the IPv6 address for a port.

Syntax

ipv6 interface address WORD<0–255>

no ipv6 interface address WORD<0–255>

Parameters

Variable	Value
WORD<0–255>	Assigns an IPv6 address to the port.

Default

None

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface enable (for a port)

Enable IPv6 route advertisement on a port.

Syntax

ipv6 interface enable

no ipv6 interface enable

default ipv6 interface enable

Parameters

None

Default

The default is disabled.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface hop-limit (for a port)

Configures the maximum number of hops before packets drop.

Syntax

ipv6 interface hop-limit <1–255>

default ipv6 interface hop-limit

Parameters

Variable	Value
<1–255>	Configures the maximum hops.

Default

The default is 64 hops.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface link-local (for a port)

Creates a link-local address for the port.

Syntax

`ipv6 interface link-local WORD<0–19>`

Parameters

Variable	Value
WORD<0–19>	Specifies the 64-bit interface ID used to calculate the actual link-local address.

Default

None.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface mac-offset

Requests a MAC for an IPv6 VLAN.

Syntax

`ipv6 interface mac-offset <0–1535>`

Parameters

Variable	Value
<0–1535>	Requests a particular MAC for an IPv6 VLAN. The system has 1536 MAC addresses. **Note:** The last four MAC addresses are reserved. You can specify a MAC offset when you configure IPv6 on a VLAN, or the system can assign a MAC address from within the available range.

Default

None

Comand mode

VLAN Interface Configuration

ipv6 interface mtu (for a port)

Configure the maximum transmission unit for the port.

Syntax

`ipv6 interface mtu <1280–9500>`

`default ipv6 interface mtu`

Parameters

Variable	Value
<1280–9500>	Configures the maximum transmission unit for the interface: 1280–1500, 1850, or 9500.

Default

The default is 1500.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface name (for a port)

Configures an interface description for the port.

Syntax

`ipv6 interface name WORD<0–255>`

Parameters

Variable	Value
WORD<0–255>	Assigns a descriptive name to the port.

Default

None.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface reachable-time (for a port)

Configures the time a neighbor is considered reachable after receiving a reachability confirmation.

Syntax

`ipv6 interface reachable-time <1–3600000>`

`default ipv6 interface reachable-time`

Parameters

Variable	Value
<1–3600000>	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation.

Default

The default is 30000.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface retransmit-timer (for a port)

Configures the time, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Syntax

ipv6 interface retransmit-timer <1-4294967295>

default ipv6 interface retransmit-timer

Parameters

Variable	Value
<1-4294967295>	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor.

Default

The default is 1000.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 interface vlan (for a port)

Configures the interface as part of an IPv6 VLAN.

Syntax

ipv6 interface vlan <1–4084>

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Interface Configuration mode

ipv6 nd

Configure the neighbor discovery parameters of the interface.

Syntax

ipv6 nd hop-limit <0–255>

ipv6 nd mtu <0–9500>

ipv6 nd reachable-time <0–3600000>

ipv6 nd retransmit-timer <0-4294967295>

default ipv6 nd hop-limit

default ipv6 nd mtu

default ipv6 nd reachable-time

default ipv6 nd retransmit-timer

no ipv6 nd hop-limit

no ipv6 nd mtu

no ipv6 nd reachable-time

no ipv6 nd retransmit-timer

Parameters

Variable	Value
hop-limit <*0–255*>	Sets the neighbor discovery hop-limit value for the interface.
mtu <*0–9500*>	Sets router advertisement MTU size.
reachable-time <*0–3600000*>	Sets router advertisement reachable time.
retransmit-timer <*0-4294967295*>	Sets router advertisement retransmit timer.

Default

Default values for the following variables are:

- ipv6 nd MTU 0
- hop limit 64

- reachable time 0
- retransmit time 0

Command mode

Interface Configuration mode

ipv6 nd dad-ns (for a port)

Configures the number of neighbor solicitation messages from duplicate address detection.

Syntax

ipv6 nd dad-ns <0–600>

default ipv6 nd dad-ns

Parameters

Variable	Value
<0–600>	Configures the number of neighbor solicitation messages from duplicate address detection. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions

Default

The default is 1.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd hop-limit (for a port)

Configure the hop limit sent in router advertisements.

Syntax

ipv6 nd hop-limit <0–255>

Parameters

Variable	Value
hop-limit <*0–255*>	Specifies the current hop limit field sent in router advertisements from this interface. The value must be the current diameter of the Internet. A value of zero indicates that the advertisement does not specify a hop-limit value.

Default

The default is 64.

Command mode

Interface Configuration mode

ipv6 nd managed-config-flag (for a port)

Enables M-bit (managed address configuration) on the router.

Syntax

`ipv6 nd managed-config-flag`

`default ipv6 nd managed-config-flag`

`no ipv6 nd managed-config-flag`

Parameters

None

Default

The default is disabled.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd mtu (for a port)

Configure the maximum transmission unit (MTU) for router advertisements.

Syntax

ipv6 nd mtu <0–9500>

Parameters

Variable	Value
mtu *<0–9500>*	Shows the MTU value sent in router advertisements on this interface. A value of zero indicates that the system sends no MTU options. Valid values are: 0, 1280–1500, 1850, or 9500.

Default

None

Command mode

Interface Configuration mode

ipv6 nd other-config-flag (for a port)

Enables the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoconfigures received information without addresses.

Syntax

ipv6 nd other-config-flag

default ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

Default

The default is disabled.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd prefix-interface (for a port)

Configures neighbor discovery prefixes IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Syntax

ipv6 nd prefix-interface WORD<0–255> [eui <1–3>] [no-advertise] [no-autoconfig] [no-onlink]

default ipv6 nd prefix-interface WORD<0–255> [no-advertise]

no ipv6 nd prefix-interface WORD<0–255> [no-advertise]

Parameters

Variable	Value
eui <*1–3*>	Specifies if extended unique identifier (EUI) is used. The values are: • (1) EUI not used • (2) EUI with Universal/Local bit (U/L) complement enabled • (3) EUI used without U/L
no-advertise	Removes the prefix from the neighbor advertisement.
no-autoconfig	Configures if the prefix is used for autonomous address configuration.
no-onlink	Configures if onlink determination uses the prefix. This value is placed in the L-bit field in the prefix information option and is a 1-bit flag.
WORD <*0–255*>	Specifies the IPv6 address prefix.

Default

The following list provides the default for the command variables:

• no-advertise: disabled

Command mode

Interface Configuration mode

ipv6 nd prefix(for a port)

Configure neighbor discovery prefixes. IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Syntax

ipv6 nd prefix WORD<0–255> [infinite] [no-advertise] [preferred-life <0-4294967295>] [valid-life <0-4294967295>]

default ipv6 nd prefix WORD<0–255> [no-advertise] [preferred-life] [valid-life]

no ipv6 nd prefix WORD<0–255> [no-advertise]

Parameters

Variable	Value
infinite	Configures the prefix as infinite.
no-advertise	Removes the prefix from the neighbor advertisement.
preferred-life *<0-4294967295>*	Configures the preferred life, in seconds. The valid range is 0-4294967295.
valid-life *<0-4294967295>*	Configures the valid life, in seconds. The valid range is 0-4294967295.

Default

The following list provides the default for the command variables:

- no-advertise: disabled
- preferred-life: 604800
- valid-life: 2592000

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd valid-life (for a port)

Mofify an existing neighbor discovery prefix. Configure the valid lifetime in seconds that indicates the length of time this prefix is advertised.

Syntax

`ipv6 nd prefix WORD<0–255> valid-life <0-4294967295>`

Parameters

Variable	Value
valid-life *<0-4294967295>*	Configures the valid lifetime in seconds that indicates the length of time this prefix is advertised. The default is 2592000. A valid lifetime is the length of time of the preferred and depreciated state of an auto configuration address.
WORD<0–255>	Specifies the IPv6 address and prefix.

Default

valid-life: 2592000

Command mode

Interface Configuration mode

ipv6 nd prefix preferred-life (for a port)

Modify an existing neighbor discovery prefix. Configure the preferred lifetime in seconds that indicates the length of time this prefix is advertised.

Syntax

`ipv6 nd prefix WORD<0–255> preferred-life <0-4294967295>`

Parameters

Variable	Value
preferred-life *<0-4294967295>*	Configures the preferred lifetime in seconds that indicates the length of time this prefix is advertised. The default value is 604800. The preferred lifetime is the length of time for the

Variable	Value
	tentative, preferred, and depreciated state of an auto configuration address.
WORD<0–255>	Specifies the IPv6 address and prefix.

Default

preferred-life: 604800

Command mode

Interface Configuration mode

ipv6 nd ra-lifetime (for a port)

Configures the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.

Syntax

ipv6 nd ra-lifetime <0–9000>

default ipv6 nd ra-lifetime

Parameters

Variable	Value
<0–9000>	Configures the router lifetime included in router advertisement. The range is 0 | <4–9000>

Default

The default is 1800.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd reachable-time (for a port)

Configure the neighbor reachable time.

Syntax

ipv6 nd reachable-time <0–3600000>

Parameters

Variable	Value
reachable-time *<0–3600000>*	Specifies a value (in milliseconds) placed in the router advertisement message sent by the router. The value zero means unspecified (by this system). Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event.

Default

None

Command mode

Interface Configuration mode

ipv6 nd retransmit-timer (for a port)

Configure the time between neighbor solicitation messages.

Syntax

`ipv6 nd retransmit-timer <0-4294967295>`

Parameters

Variable	Value
retransmit-timer *<0-4294967295>*	Specifies a value (in milliseconds) placed in the retransmit timer field in the router advertisement message sent from this interface. The value zero means unspecified (by this system). The value configures the amount of time the system waits for the transmission to occur.

Default

None

Command mode

Interface Configuration mode

ipv6 nd rtr-advert-max-interval (for a port)

Configures the maximum time allowed between sending unsolicited multicast router advertisements.

Syntax

ipv6 nd rtr-advert-max-interval <4–1800>

default ipv6 nd rtr-advert-max-interval

Parameters

Variable	Value
<4–1800>	Specifies the maximum interval value.

Default

The default is 600.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd rtr-advert-min-interval (for a port)

Configures the minimum time allowed between sending unsolicited multicast router advertisements from the interface.

Syntax

ipv6 nd rtr-advert-min-interval <3–1350>

default ipv6 nd rtr-advert-min-interval

Parameters

Variable	Value
<3–1350>	Configures the minimum time, in seconds.

Default

The default is 200.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 nd send-ra (for a port)

Enables or disables periodic router advertisement messages.

Syntax

ipv6 nd send-ra

default ipv6 nd send-ra

no ipv6 nd send-ra

Parameters

None

Default

The default is enabled.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ipv6 ospf (for a port or VLAN)

Configure OSPFv3 on an interface (VLAN or Ethernet port).

Syntax

ipv6 ospf area {A.B.C.D} [dead-interval <1–65535>] [network <eth| nbma|p2mp|p2p|passive>]

ipv6 ospf cost <0–65535> [priority <0–255>]

ipv6 ospf dead-interval <1–65535>

ipv6 ospf enable

ipv6 ospf hello-interval <1–65535>

ipv6 ospf nbma-nbr WORD<0–43> <0–255>

ipv6 ospf nbma-nbr WORD<0–43> [priority <0–255>]

ipv6 ospf poll-interval <0-65535>

ipv6 ospf priority <0–255>

ipv6 ospf retransmit-interval <1-1800>

ipv6 ospf transit-delay <1-1800>

default ipv6 ospf cost [priority]

default ipv6 ospf dead-interval

default ipv6 ospf [enable]

default ipv6 ospf hello-interval

default ipv6 ospf nbma-nbr WORD<0-43>

default ipv6 ospf poll-interval

default ipv6 ospf priority

default ipv6 ospf retransmit-interval

default ipv6 ospf transit-delay

no ipv6 ospf [enable]

no ipv6 ospf nbma-nbr WORD<0-43>

Parameters

Variable	Value
area {A.B.C.D}	Creates an IPv6 OSPF area.
cost *<0–65535>*	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements.
dead-interval *<1–65535>*	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down.
enable	Enables the OSPF on the IPv6 interface.
hello-interval *<1–65535>*	Specifies the hello interval, in seconds, for hello packets sent between switches for a virtual interface in an OSPF area.
nbma-nbr *WORD<0–43>*	Configures an NBMA neighbor. *WORD<0–43>* specifies the IPv6 address. Use priority *<0–255>* to change an existing priority value for an NBMA neighbor. Use *<0–255>* to assign the priority value when you create the neighbor.

Variable	Value
network <eth|nbma|p2mp|p2p|passive>	Configures the type of interface as one of the following: • eth: broadcast • nbma: NBMA • p2mp: point-to-multipoint • p2p:point-to-point • passive:passive interface
poll-interval <*0-65535*>	Configures the polling interval for the OSPF interface in seconds.
priority <*0–255*>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priorityis used only during election of the designated router and backup designated router.
retransmit-interval <*1–1800*>	Specifies the retransmit interval, in seconds, for link-state advertisements.
transit-delay <*1–1800*>	Specifies the transit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface.

Default

The following list provides the default values:

- cost: 1
- dead-interval:40
- hello-interval:10
- poll-interval: 120
- priority: 1
- retransmit-interval:5
- transit-delay:1

Command mode

Interface Configuration mode

ipv6 prefix-list

Use prefix lists to allow or deny specific route updates. A prefix list policy specifies route prefixes to match. When there is a match, the route is used.

Configure a prefix list and apply the list to a route policy.

Syntax

ipv6 prefix-list WORD<1-64> WORD<1-256> [ge <0- 128>] [le <0-128>]

ipv6 prefix-list WORD<1-64> name WORD<1-64>

no ipv6 prefix-list WORD<1-64> [WORD<1-256>]

Parameters

Variable	Value
*WORD<1-64> WORD<1-256>*ge *<0- 128>* le *<0-128>*	Adds a prefix entry to the prefix list. • *WORD<1-64>* is the prefix-list name. • *WORD<1-256>* is the IPv6 address and length. • <ge|le>*<0- 128>* is the minimum and maximum length to match. Lower bound and higher bound mask lengths together can define a range of networks.
name *WORD<1-64>*	Renames the specified prefix list. The name length is from 1 to 64 characters.

Default

None

Command mode

Global Configuration mode

ipv6 redistribute

Enable redistribution to redistribute IPv6 routes into an OSPFv3 routing domain.

Syntax

ipv6 redistribute {bgp|direct|static} [enable]

default ipv6 redistribute {bgp|direct|static} [enable]

no ipv6 redistribute {bgp|direct|static} [enable]

Parameters

Variable	Value
{bgp|direct|static}	Specifies the type of IPv6 route to redistribute to the OSPFv3 routing domain.
enable	Enables redistribution.

Default

The default is disabled.

Command mode

OSPF Router Configuration mode

ipv6 route

Configures a static route to destination IPv6 address prefixes.

Syntax

ipv6 route WORD<0-46> [cost <1-65535>] [next-hop WORD<0-46>] [port {slot/port}] [preference <1–255>] [tunnel <1–2000>] [vlan <1–4084>]

ipv6 route WORD<0-46> enable [next-hop WORD<0-46>] [port {slot/port}] [tunnel <1–2000>] [vlan <1–4084>]

ipv6 route WORD<0-46> preference <1–255> [next-hop WORD<0-46>] [port {slot/port}] [tunnel <1–2000>] [vlan <1–4084>]

default ipv6 route WORD<0-46> [enable] [next-hop WORD<0-46>] [port {slot/port}] [tunnel <1–2000>] [vlan <1–4084>]

default ipv6 route WORD<0-46> preference [next-hop WORD<0-46>] [port {slot/port}] [preference <1–255>] [tunnel <1–2000>] [vlan <1–4084>]

no ipv6 route WORD<0-46> [enable] [next-hop WORD<0-46>] [port {slot/port}] [tunnel <1–2000>] [vlan <1–4084>]

Parameters

Variable	Value
cost <*1-65535*>	Specifies the cost or distance ratio to reach the destination for this node.

Variable	Value
enable	Enables the static route on the port.
next-hop *WORD<0-46>*	Specifies the IPv6 address of the next hop on this route. You do not need to specify the next hop if the devices directly connect to one another. Configure the next hop if the two nodes do not share the same network prefix but reside on the same link.
port {slot/port}	Specifies the port to which this entry applies. You must specify the port if the next hop is a link-local address.
preference *<1–255>*	Specifies the routing preference of the destination IPv6 address.
tunnel *<1–2000>*	Specifies the tunnel to which this entry applies.
vlan *<1–4084>*	Specifies the VLAN to which this entry applies. You must specify the VLAN if the next hop is a link-local address.
WORD<0-46>	Specifies the IPv6 destination network address.

Default

The default cost is 1. The default state for a new static route is enable. The default preference is 5.

Command mode

Global Configuration mode

ipv6 route static

Enables static routes globally. If you disable static routes globally, the system removes all enabled static routes from the RTM and does not add new static routes to the RTM.

Syntax

`ipv6 route static enable`

`default ipv6 route static enable`

`no ipv6 route static enable`

Parameters

Variable	Value
enable	Enables the static routes globally.
static	Modifies IPv6 static route parameters.

Default

The default is enabled.

Command mode

Global Configuration mode

ipv6 router-id

Configure the OSPF router ID.

Syntax

ipv6 router-id {A.B.C.D}

default ipv6 router-id

Parameters

Variable	Value
{A.B.C.D}	Specifies the IPv4 address for the router ID.

Default

None.

Command mode

OSPF Router Configuration mode

ipv6 rvs-path-chk

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IPv6 source addresses into a network.

Syntax

ipv6 rvs-path-chk [mode <exist-only|strict>]

default ipv6 rvs-path-chk [mode]

no ipv6 rvs-path-chk

Parameters

Variable	Value
mode <exist-only|strict>	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source address of the incoming packet exists in the routing table. If the source entry is found, the packet is forwarded as usual; otherwise, the packet is discarded. In strict mode, reverse path checking checks whether the source address for the incoming packet exists in the routing table. If the source entry is found, reverse path checking further checks if the source IP interface address matches the packet incoming interface address. If they match, the packet is forwarded as usual, otherwise, the packet is discarded.

Default

Reverse path checking is disabled by default. If you enable reverse path checking, the default mode is exist-only.

Command mode

GigabitEthernet Interface Configuration mode and VLAN Interface Configuration mode

ipv6 send-trap enable

Configures Virtual Router Redundancy Protocol (VRRP) notification control.

Syntax

ipv6 send-trap [enable]

default ipv6 send-trap [enable]

no ipv6 send-trap [enable]

Parameters

None

Default

Generation of SNMP traps for VRRP events is enabled.

Command mode

VRRP Router Configuration mode

ipv6 tunnel

Configures a tunnel for IPv6 VLANs or brouter ports to communicate through an IPv4 network.

Syntax

ipv6 tunnel <1–2000> hop-limit <0–255>

ipv6 tunnel <1–2000> source {A.B.C.D} address WORD<0-46> destination {A.B.C.D}

default ipv6 tunnel <1–2000> [hop-limit]

no ipv6 tunnel <1–2000>

Parameters

Variable	Value
<1–2000>	Specifies the tunnel ID.
address *WORD<0-46>*	Specifies the IPv6 address and length for the local VLAN or brouter port.
destination{A.B.C.D}	Configures the address of the remote endpoint of the tunnel.
hop-limit *<0–255>*	Configures the maximum number of hops in the tunnel.
source {A.B.C.D}	Configures the address of the local endpoint of the tunnel, or 0.0.0.0 (for IPv4) or :: (for IPv6) if the device is free to choose its addresses at tunnel establishment.

Default

The default hop-limit is 255.

Command mode

Global Configuration mode

ipv6 tunnel (for OSPF)

Configure OSPF parameters for an IPv6 tunnel.

Syntax

ipv6 tunnel <1–2000> area {A.B.C.D} [dead-interval <1–65535>] [hello-interval <1–65535>] [metric <0–65535>] [priority <0–255>] [retransmit-interval <1–1800>] [transmit-delay <1–1800>]

ipv6 tunnel <1–2000> enable [dead-interval <1–65535>] [hello-interval <1–65535>] [metric <0–65535>] [priority <0–255>] [retransmit-interval <1–1800>] [transmit-delay <1–1800>]

ipv6 tunnel <1–2000> poll-interval <0–65535>

default ipv6 tunnel <1–2000> [enable] [dead-interval] [hello-interval] [metric] [priority] [retransmit-interval] [transmit-delay]

no ipv6 tunnel <1–2000> [enable]

Parameters

Variable	Value
<1–2000>	Specifies the tunnel ID.
{A.B.C.D}	Specifies the area address.
dead-interval *<1–65535>*	Specifies the dead interval, as the number of seconds to wait before determining the OSPF router is down.
hello-interval *<1–65535>*	Specifies the hello interval, in seconds, for hello packets sent between switches for an interface in an OSPF area.
metric *<0–65535>*	Configures the OSPF metric for the tunnel. The switch advertises the metric in router link advertisements.
poll-interval *<0–65535>*	Configures the polling interval, in seconds, for the OSPF tunnel.
priority *<0–255>*	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot

Variable	Value
	become either the designated router or a backup.
retransmit-interval <*1–1800*>	Specifies the retransmit interval, in seconds, for link-state advertisements.
transmit-delay <*1–1800*>	Specifies the transmit-delay interval, in seconds, required to transmit a link-state update packet over the virtual interface.

Default

The following list provides the default values:

- dead-interval: 40
- hello-interval: 10
- poll-interval: 120
- priority: 1
- metric: 100
- retransmit-interval: 5
- transmit-delay:1

Command mode

OSPF Router Configuration mode

ipv6 vrrp

Configures VRRP to provide fast failover of a default router for IPv6 LAN hosts. VRRP supports a virtual IPv6 address shared between two or more routers that connect the common subnet to the enterprise network. VRRP for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

Syntax

ipv6 vrrp <1-255> enable

ipv6 vrrp <1-255> accept-mode enable

ipv6 vrrp <1-255> action <none|preempt>

ipv6 vrrp <1-255> adver-int <1-40>

ipv6 vrrp <1-255> backup-master enable

ipv6 vrrp <1-255> critical-ipv6-addr WORD<0-46> [critical ipv6 enable]

```
ipv6 vrrp <1-255> fast-adv enable [fast-adv-int <200-1000>]
ipv6 vrrp <1-255> holddown-timer <0-21600>
ipv6 vrrp <1-255> priority <1-255>
default ipv6 vrrp <1-255> [enable]
default ipv6 vrrp <1-255> accept-mode enable
default ipv6 vrrp <1-255> action
default ipv6 vrrp <1-255> adver-int
default ipv6 vrrp <1-255> backup-master enable
default ipv6 vrrp <1-255> critical-ipv6-addr [critical ipv6 enable]
default ipv6 vrrp <1-255> fast-adv enable [fast-adv-int]
default ipv6 vrrp <1-255> holddown-timer
default ipv6 vrrp <1-255> priority
no ipv6 vrrp <1-255> [enable]
no ipv6 vrrp <1-255> accept-mode enable
no ipv6 vrrp <1-255> backup-master enable
no ipv6 vrrp <1-255> critical ipv6 enable
no ipv6 vrrp <1-255> fast-adv enable
```

Parameters

Variable	Value
<1–255>	Specifies a number that uniquely identifies a virtual router on an interface. The virtual router acts as the default router for one or more assigned addresses.
accept-mode enable	Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner.
action <none|preempt>	Lists options to override the holddown timer manually and force preemption: • none does not override the timer. • preempt preempts the timer. This parameter applies only if the holddown timer is active.

Variable	Value
adver-int <*1-40*>	Specifies the time interval, in seconds, between sending advertisement messages. Only the master router sends advertisements. The default is 1.
backup-master enable	Uses the backup VRRP switch for traffic forwarding. This option reduces the traffic on the IST link.
critical-ip enable	Enables or disables the use of critical IP. When disabled, the VRRP ignores the availability of the address configured as critical IP. This address must be a local address.
critical-ip-addr *WORD<0-46>*	Specifies an IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding.
enable	Enables IPv6 VRRP.
fast-adv enable	Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used.
fast-adv-int <*200-1000*>	Configures the interval between VRRP advertisement messages. You must configure the same value on all participating routers. This unit of measure must be in multiples of 200 milliseconds.
holddown-timer<*0-21600*>	Configures the amount of time, in seconds, to wait before preempting the current VRRP master.
priority <*1-255*>	Specifies the priority value used by this VRRP router. The value 255 is reserved for the router that owns the IP addresses associated with the virtual router.

Default

The following list provides the default values for the applicable command parameters:

- accept-mode enable: disabled
- adver-int: 1
- backup-master enable: disabled
- critical-ip enable: disabled
- enable: disabled
- fast-adv enable: disabled
- fast-adv-int: 200
- holddown-timer: 0
- priority: 100

Command mode

Interface Configuration mode

ipv6 vrrp address

Specifies a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

Syntax

ipv6 vrrp address <1-255> link-local WORD<0-127>

default ipv6 vrrp address <1-255>

no ipv6 vrrp address <1-255>

Parameters

Variable	Value
<1-255>	Specifies the virtual router ID. The virtual router acts as the default router for one or more associated addresses.
link-local *WORD<0-127>*	Specifies a link-local IPv6 address to associate with the virtual router.

Default

None

Command mode

Interface Configuration mode

show ipv6 address

View IPv6 address entries.

Syntax

show ipv6 address interface

show ipv6 address interface gigabitethernet [{slot/port[-slot/port][,...]}]

show ipv6 address interface ip WORD<0–46>

show ipv6 address interface vlan [<1–4084>]

show ipv6 address interface tunnel <1–2000>

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
tunnel *<1–2000>*	Displays the address entries specific to a tunnel ID.
WORD<0–46>	Specifies an IPv6 address.

Default

None

Command mode

Privileged EXEC mode

show ipv6 dcache

Displays the destination cache to see next-hop addresses for destinations. The destination cache is only populated or updated when IPv6 packets originate locally on the central processor of the switch.

Syntax

show ipv6 dcache [gigabitethernet {slot/port}] [mgmtethernet {slot/port}] [tunnel <1–2000>] [vlan <1–4084>]

Parameters

Variable	Value
<1–2000>	Specifies the tunnel ID.
<1–4084>	Specifies the VLAN ID.
{slot/port}	Identifies the slot and port.

Default

None

Command mode

Privileged EXEC mode

show ipv6 dhcp-relay

Display IPv6 DHCP Relay information to show relay information about DHCP routes and counters.

Syntax

show ipv6 dhcp-relay counters

show ipv6 dhcp-relay fwd-path

show ipv6 dhcp-relay interface [gigabitethernet {slot/port[-slot/port][,...]}] [vlan <1–4084>]

Parameters

Variable	Value
counters	Displays the count of DHCP Relay requests and replies.
fwd-path	Displays information about DHCP Relay forward paths.
gigabitethernet {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
vlan <*1–4084*>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show ipv6 forwarding

Show IPv6 forwarding information.

Syntax

`show ipv6 forwarding`

Parameters

None

Default

Disabled

Command mode

Privileged EXEC mode

show ipv6 global

Show global IPv6 configuration information.

Syntax

`show ipv6 global`

Parameters

None

Default

Following are default values in the output for **`show ipv6`** :

- forwarding, disable
- default-hop-cnt, 64
- number-of-interfaces, 0
- icmp-error-interval, 1000
- icmp-unreach-msg, disable
- icmp-redirect-msg, disable
- static-route-admin-status, enable

Command mode

Privileged EXEC mode

show ipv6 interface

Show IPv6 information for all or specific interfaces.

Syntax

show ipv6 interface gigabitethernet [{slot/port[-slot/port][,...]}]

show ipv6 interface icmpstatistics gigabitEthernet [{slot/port[-slot/port][,...]}]

show ipv6 interface statistics gigabitEthernet [{slot/port[-slot/port][,...]}]

show ipv6 interface mgmtEthernet [{slot/port[-slot/port][,...]}]

show ipv6 interface icmpstatistics mgmtEthernet [{slot/port[-slot/port][,...]}]

show ipv6 interface statistics mgmtEthernet [{slot/port[-slot/port][,...]}]

show ipv6 interface tunnel <1–2000>

show ipv6 interface icmpstatistics tunnel <1-2000>

show ipv6 interface statistics tunnel <1–2000>

show ipv6 interface vlan [<1–4084>]

show ipv6 interface icmpstatistics [vlan <1–4084>]

show ipv6 interface statistics vlan <1–4084>

show ipv6 interface icmpstatistics

show ipv6 interface statistics

Parameters

Variable	Value
gigabitEthernet {slot/port[-slot/port][,...]}	Displays IPv6 interface information for gigabitEthernet as one of the following: • a single slot and port (3/1) • a range of slots and ports (3/2-3/4, • a series of slots and ports (3/2,5/3,6/2)

Variable	Value
mgmtEthernet {slot/port[-slot/port][,...]}	Displays IPv6 interface information for mgmtEthernet as one of the following: • a single slot and port (3/1) • a range of slots and ports (3/2-3/4, • a series of slots and ports (3/2,5/3,6/2)
tunnel <1–2000>	Displays IPv6 interface information for a tunnel. The tunnel ID is expressed as a value from 1 to 2000.
vlan <1–4084>	Displays IPv6 interface information for a VLAN. The VLAN ID is expressed as a value from 1 to 4084.
icmpstatistics [gigabitEthernet | mgmtEthernet | tunnel | vlan]	Shows IPv6 ICMP statistics for the interface as follows: • gigabitEthernet—displays interface gigabitEthernet configurations • mgmtEthernet—displays interface mgmtEthernet configurations • tunnel—displays interface tunnel configurations • vlan —displays vlan interface configurations
statistics [gigabitEthernet | mgmtEthernet | tunnel | vlan]	Shows IPv6 interface statistics as follows: • gigabitEthernet—displays interface gigabitEthernet configurations • mgmtEthernet—displays interface mgmtEthernet configurations • tunnel—displays interface tunnel configurations • vlan —displays vlan interface configurations

Default

None

Command mode

Privileged EXEC mode

show ipv6 nd

View neighbor discovery interface configuration.

Syntax

show ipv6 nd interface gigabitethernet [{slot/port[-slot/port][,...]}]

show ipv6 nd interface vlan [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show ipv6 nd-prefix

View all configured neighbor discovery prefixes.

Syntax

show ipv6 nd-prefix [detail]

show ipv6 nd-prefix interface gigabitethernet [{slot/port[-slot/port][,...]}]

show ipv6 nd-prefix interface vlan [<1–4084>]

show ipv6 nd-prefix vlan [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
detail	Shows detailed information.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show ipv6 neighbor

View entries in the neighbor cache.

Syntax

show ipv6 neighbor

show ipv6 neighbor interface gigbitethernet {slot/port}

show ipv6 neighbor interface mgmtEthernet {slot/port}

show ipv6 neighbor interface mlt <1–512>

show ipv6 neighbor interface vlan <1–4084>

show ipv6 neighbor type <1–4>

show ipv6 neighbor WORD<0–46>

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.
<1–4084>	Specifies the VLAN ID.
{slot/port}	Identifies the slot and port for the interface.

Variable	Value
type <*1–4*>	Specifies the type of mapping: • 1: other • 2: dynamic • 3: static • 4: local
WORD<0–46>	Specifies the neighbor address.

Default

None

Command mode

Privileged EXEC mode

show ipv6 ospf

Show the IPv6 OSPFv3 global configuration.

Syntax

`show ipv6 ospf`

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 ospf area

Show the IPv6 OSPFv3 area configuration.

Syntax

`show ipv6 ospf area`

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 ospf area-range

Show the IPv6 OSPFv3 range configuration.

Syntax

show ipv6 ospf area-range

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 ospf ase

Show the IPv6 OSPFv3 as-external LSAs.

Syntax

show ipv6 ospf ase [metric-type <1–2>]

Parameters

Variable	Value
metric-type <*1–2*>	Specifies the external type.

Default

None

Command mode

User EXEC mode

show ipv6 ospf int-timers

Show the IPv6 OSPFv3 interface timers.

Syntax

show ipv6 ospf int-timers

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 ospf interface

Show the IPv6 OSPFv3 interface configuration.

Syntax

show ipv6 ospf interface [gigabitEthernet {slot/port}] [vlan <1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port]	Specifies the slot and port.

Default

None

Command mode

User EXEC mode

show ipv6 ospf lsdb

Show the IPv6 OSPFv3 Link-state database configuration.

Syntax

show ipv6 ospf lsdb [adv-rtr {A.B.C.D}] [area {A.B.C.D}] [detail] [interface gigabitEthernet {slot/port}] [interface vlan <1–4084>] [lsa-type <1–9>] [lsid <0-4294967295>] [scope <1–3>] [tunnel <1–2000>]

Parameters

Variable	Value
adv-rtr {A.B.C.D}	Shows information for the specified advertising router.
area {A.B.C.D}	Shows information for the specified area.
detail	Shows information beyond the basic details.
interface gigabitEthernet {slot/port}	Shows information for the specified interface.
interface vlan <1–4084>	Shows information on the specified interface.
lsa-type <*1–9*>	Shows information for the specified LSA type.
lsid <*0-4294967295*>	Shows information for the specified link-state ID.
scope <*1–3*>	Shows information for the specified scope.
tunnel <*1–2000*>	Shows information for the specified tunnel.

Default

None

Command mode

User EXEC mode

show ipv6 ospf nbma-nbr interface

Show the IPv6 OSPFv3 NBMA neighbor configuration.

Syntax

show ipv6 ospf nbma-nbr interface gigabitEthernet {slot/port} [WORD<1–46>]

show ipv6 ospf nbma-nbr interface vlan <1–4084> [WORD<1–46>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port}	Specifies the slot and port.
WORD<1–46>	Specifies an IPv6 address.

Default

None

Command mode

User EXEC mode

show ipv6 ospf neighbor

Show the IPv6 OSPFv3 neighbor configuration.

Syntax

show ipv6 ospf neighbor

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 ospf redistribute

Show the IPv6 OSPFv3 redistribution configuration.

Syntax

show ipv6 ospf redistribute

Parameters

None

Default

Disabled

Command mode

User EXEC mode

show ipv6 ospf statistics

Show the IPv6 OSPFv3 statistics.

Syntax

show ipv6 ospf statistics

Parameters

None

Default

None

Command mode

User EXEC mode

show ipv6 prefix-list

Show IPv6 prefix-list information.

Syntax

show ipv6 prefix-list

show ipv6 prefix-list prefix WORD<1–256>

show ipv6 prefix-list WORD<1–64>

Parameters

Variable	Value
prefix-list	Shows IPv6 prefix-list information.
prefix	Specifies the prefix.
WORD<1–64>	Specifies the prefix-list name.

Default

None

Command mode

User EXEC mode

show ipv6 route

Show IPv6 routes for the switch.

Syntax

show ipv6 route [count-summary] [dest WORD<0–46>] [gigabitethernet {slot/port}] [next-hop WORD<0–46>] [static] [tunnel <1–2000>] [vlan <1–4084>]

Parameters

Variable	Value
count-summary	Shows the total number of OSPF, RIP, BGP, static, and local routes.
dest *WORD<0–46>*	Shows the route to a specific IPv6 address.
next-hop *WORD<0–46>*	Shows the route to a specific IPv6 next hop.
{slot/port}	Identifies the slot and port for the interface.
static	Shows static IPv6 routes.
tunnel *<1–2147477248>*	Shows route entries for a specific tunnel ID.

Variable	Value
vlan <*1–4084*>	Shows route entries for a specific VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show ipv6 tcp

You can display IPv6 TCP information.

When you view TCP information you can

- check the health of connections, from the switch perspective, as they traverse the network
- detect intermittent connectivity
- detect attacks on resources
- determine which applications are active by checking the port numbers
- view statistics about TCP connections

Syntax

`show ipv6 tcp <connections|listener|properties|statistics>`

Parameters

Variable	Value
connections	Displays IPv6 TCP connection table information that includes: • local port • remote port • local address • remote address • state
listener	Displays IPv6 TCP listener table information that includes: • local port • local address

Variable	Value
properties	Displays IPv6 TCP global properties information that includes: • RtoAlgorithm — the timeout value used for retransmitting unacknowledged octets • RtoMin —the minimum time, in milliseconds, permitted by a TCP implementation for the retransmission timeout • RtoMax — the maximum time (in milliseconds) permitted by a TCP implementation for the retransmissions timeout • MaxConn — the maximum connections for the device
statistics	Displays IPv6 TCP global statistics information that includes: • ActiveOpens • PassiveOpens • AttemptFails • EstabResets • CurrEstab • InSegs • OutSegs • RetransSegs • InErrs • OutRsts • HCInSegs • HCOutSegs

Default

None

Command mode

Privileged EXEC mode

show ipv6 trace

Show the status of IPv6 trace commands.

Syntax

`show ipv6 trace <base|forwarding|nd|ospf|rtm|transport>`

Parameters

Variable	Value
<base|forwarding|nd|ospf|rtm|transport>	Shows the status for the selected type of trace command.

Default

None

Command mode

Privileged EXEC mode

show ipv6 tunnel

Shows information about configured IPv6 tunnels, for example, operational state or addresses.

Syntax

`show ipv6 tunnel [<1–2000>] [detail] [local {A.B.C.D}] [remote {A.B.C.D}]`

Parameters

Variable	Value
<1–2000>	Shows configuration information for a specific tunnel ID.
detail	Shows detailed configuration information, for example, the operational status and origin.
local {A.B.C.D}	Shows configuration information for a specific local endpoint address.

Variable	Value
remote {A.B.C.D}	Shows configuration information for a specific remote endpoint address.

Default

None

Command mode

Privileged EXEC mode

show ipv6 udp

Show IPv6 User Datagram Protocol (UDP) information.

Syntax

show ipv6 udp

show ipv6 udp endpoints

show ipv6 udp local_addr WORD<0–128> [{slot/port}]

show ipv6 udp remote_addr WORD<0–128> [{slot/port}]

Parameters

Variable	Value
endpoints	Shows IPv6 UDP information for the endpoints.
local_addr *WORD<0–128> [{slot/port}]*	Shows IPv6 UDP information for a local IPv6 address or slot and port.
remote_addr *WORD<0–128> [{slot/port}]*	Shows IPv6 UDP information for a remote IPv6 address or slot and port.

Default

None

Command mode

Privileged EXEC mode

show ipv6 vrrp

Shows the global status of VRRP for IPv6.

Syntax

show ipv6 vrrp

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ipv6 vrrp address

Displays address information for a specific link-local address or virtual router ID.

Syntax

show ipv6 vrrp address

show ipv6 vrrp address link-local WORD<0–127>

show ipv6 vrrp address vrid <1–255>

Parameters

Variable	Value
link-local *WORD<0–127>*	Displays information by link-local IPv6 address.
vrid *<1–255>*	Displays information by virtual router ID.

Default

None

Command mode

Privileged EXEC mode

show ipv6 vrrp interface

Shows the extended VRRP configuration for all interfaces or for a specific interface.

Syntax

show ipv6 vrrp interface [verbose]

show ipv6 vrrp interface gigabitethernet [{slot/port[-slot/port][,...]}] [verbose]

show ipv6 vrrp interface vlan [<1–4084>] [verbose]

show ipv6 vrrp interface vrid <1–255> [verbose]

Parameters

Variable	Value
<1–255>	Displays information by virtual router ID.
<1-4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
verbose	Displays extended information.

Default

None

Command mode

Privileged EXEC mode

show ipv6 vrrp interface gigabitethernet statistics

Shows the IPv6 gigabitEthernet interface statistics.

Syntax

show ipv6 vrrp interface gigabitethernet statistics [slot/port[-slot/port][,....]] [verbose]

Parameters

Variable	Value
statistics	Displays the IPv6 interface gigabitEthernet statistics.
statistics*[slot/port[-slot/port][,....]]*	Displays the IPv6 statistics for a port.
verbose	Displays extended information.

Default

None

Command mode

User EXEC mode

show ipv6 vrrp statistics

Views VRRP for IPv6 statistics to manage network performance.

Syntax

`show ipv6 vrrp statistics [link-local WORD<0-127>] [vrid <1-255>]`

Parameters

Variable	Value
<1-255>	Displays information by virtual router ID.
WORD<0-127>	Displays information by link-local IPv6 address.

Default

None

Command mode

Privileged EXEC mode

Chapter 11: Link aggregation, MLT, and SMLT commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to configure link aggregation and MultiLink trunking (MLT) on the Avaya Virtual Services Platform 9000.

hash-calc getmltindex traffic-type

View the MLT port calculated by the MLT hash algorithm to determine through which MLT port a packet will exit the system.

Syntax

hash-calc getmltindex traffic-type <ipv4|ipv6|non-ip> dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512>

hash-calc getmltindex traffic-type <ipv4|ipv6|non-ip> dest-val WORD<1-1536> src-val WORD<1-1536> mltID <1-512> [dst-port <0-65535>] [src-port <0-65535>]

Parameters

Variable	Value
dest-val *WORD<1–1536>*	Specifies the destination address in the range of 1 to 1536. The source and destination addresses cannot have the same value.
src-val *WORD<1–1536>*	Specifies the source address in the range from 1–1536. The source and destination addresses cannot have the same value.
dst-port|src-port *<0–65535>*	Specifies the destination port or the source port. The value ranges from 0 to 65535.
mltID *<1–512>*	Specifies the MLT ID. The value ranges from 1 to 512.
traffic-type *{ipv4|ipv6|non-ip}*	The type of traffic. Specifies ipv4, ipv6 or non-ip.

Default

None

Command mode

Privileged EXEC mode

ist enable

Enable an interswitch trunk.

Syntax

ist enable

default ist enable

no ist enable

Parameters

Variable	Value
enable	Enables the interswitch trunk.

Default

The default is disabled.

Command mode

MLT Interface Configuration mode

ist peer-ip

Create an interswitch trunk from an existing MLT.

Syntax

ist peer-ip <A.B.C.D> vlan <1–4084>

default ist peer-ip

no ist peer-ip

Parameters

Variable	Value
<A.B.C.D>	Specify the peer IP address—the IP address of the IST VLAN on the other aggregation switch.
<1–4084>	Specify the VLAN ID.

Default

The default is disabled.

Command mode

MLT Interface Configuration mode

lacp

Configure LACP parameters globally. When the LACP system priority is set globally, it applies to all LACP-enabled aggregators and ports.

Syntax

`lacp`

Parameters

Variable	Value
`aggr-wait-time` *<200–2000>*	Sets the aggregation wait time (in milliseconds) globally. The default value is 2000.
`enable`	Enables LACP globally. To disable LACP globally, use the **no** operator to remove this configuration. To set this option to the default value, use the **`default`** operator with the command.
`fast-periodic-time` *<200–20000>*	Sets the fast-periodic time (in milliseconds) globally. The default is 20000 ms.
`slow-periodic-time` *<10000–30000>*	Sets the slow periodic time globally. The default value is 1000 ms.
`smlt-sys-id <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the LACP system ID globally. Enter a MAC address in the following format: 0x00:0x00:0x00:0x00:0x00:0x00.
`system-priority` <0-65535>	Sets the global LACP system priority. The default value is 32768.

Variable	Value
timeout-scale *<2-10>*	Sets the timeout scale globally. The default value is 3. To set this option to the default value, use the **default** operator with the command.

Default

The default is disabled.

Command mode

Global Configuration mode

lacp enable (globally)

Configure LACP on a port to enable or disable LACP on the selected ports.

Syntax

lacp enable

Parameters

Variable	Value
enable	Enables LACP on the port.

Default

The default is disabled.

Command mode

Global Configuration mode

Related commands

Variable	Value
aggregation enable	Sets the port as aggregatable. Use the **no** operator to remove this configuration. To set this option to the default value, use the **default** operator with the command.
aggr-wait-time <200–2000>	Sets the aggregation wait time (in milliseconds) for this port. The default value is 2000.
fast-periodic-time <200–20000>	Sets the fast-periodic time (in milliseconds) for this port. The default is 1000 ms.
key <0–65535>	Sets the aggregation key for this port.

Variable	Value
`mode {active, passive}`	Sets the LACP mode to be active or passive.
`partner-key <0–65535>`	Sets the partner administrative key.
`partner-port <0–65535>`	Sets the partner administrative port value.
`partner-port-priority <0–65535>`	Sets the partner administrative port priority value.
`partner-state <0x00–0xff>`	Sets the partner administrative state bitmask. Specify the partner administrative state bitmap in the range 0x0-0xff. The bit to state mapping is Exp, Def, Dis, Col, Syn, Agg, Time, and Act. For example, to set the two partner-state parameters • Act = true • Agg = true specify a value of 0x05 (bitmap = 00000101).
`partner-system-id <0x00:0x00:0x00:0x00:0x00:0x00>`	Sets the partner administrative system ID. Specify a MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00.
`partner-system-priority <0–65535>`	Sets the partner administrative system priority value.
`priority <0–65535>`	Sets the port priority. The default value is 32768. To set this option to the default value, use the **`default`** operator with the command.
`slow-periodic-time <10000-30000>`	Sets the slow periodic time for this port. The default is 30000 ms. To set this option to the default value, use the **`default`** operator with the command.
`system-priority <0-65535>`	Sets the system priority for this port. The default value is 32768.
`timeout-scale <2-10>`	Sets a timeout scale for this port. The default value is 3. To set this option to the default value, use the **`default`** operator with the command.
`timeout-time {long,short} [timeout-scale <2-10>]`	Sets the timeout to either long or short. To set this option to the default value, use the **`default`** operator with the command.

lacp enable key

Configure an MLT with LACP to use the dynamic link aggregation function.

Syntax

lacp enable key <0–512>

Parameters

Variables	Value
key <0–512>	Sets LACP aggregator key for a specific MLT. • *<0–512>* is the LACP actor admin key.

Default

None

Command mode

Global Configuration mode

lacp enable (on an MLT)

Configure a MultiLink Trunking (MLT) with Link Aggregation Control Protocol (LACP) to use the dynamic link aggregation function.

Syntax

lacp enable

lacp key <0–512>

lacp system-priority <0–65535>

default lacp enable

default lacp key

default lacp system-priority

no lacp enable

no lacp

Parameters

Variable	Value
enable	Enables LACP on the MLT interface.
key *<0–512>*	Sets the LACP aggregator key for a specific MLT. *<0–512>* specifies the LACP actor admin key.

Variable	Value
system-priority <*0-65535*>	Sets the LACP system priority for a specific MLT. <*0–65535*> specifies the system priority.

Default

The default is disabled.

The default key value is 0.

The default system-priority is 32768

Command mode

MLT Interface mode

mlt

Configure an MLT to set up MLTs on the switch.

Syntax

`mlt <1–512>`

Parameters

Variable	Value
enable	Creates and enables a new MLT.
encapsulation dot1q	Sets encapsulation. **`dot1q`** enables trunking on the MLT.
member*{slot/port[-slot/port][,...]}*	Adds ports to this MLT.
<*1–512*>	Specifies the MLT ID in the range of 1–512.
name <*0-20*>	Changes the name for this MLT in the range of 0–20 characters.
vlan <*1–4084*>	Specifies a VLAN ID to add to this MLT.

Default

None

Command mode

Global Configuration mode

mlt member

Add ports to an MLT LAG to add an existing VLAN to a link aggregation configuration.

Syntax

`mlt <1-512> member {slot/port [-slot/port][,...]} vlan <1-4084>`

Parameters

Variable	Value
<1-512>	Specifies the MLT ID in the range of 1 to 512.
{slot/port [-slot/port][,...]}	Specifies the port and the slot number.
vlan *<1-4084>*	Specifies the VLAN ID in the range of 1 to 4084.

Default

None

Command mode

Global Configuration mode

monitor mlt error collision

Monitor MultiLink Trunking (MLT) collision error information.

Syntax

`monitor mlt error collision`

`monitor mlt error collision <1–512>`

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.

Default

None

Command mode

Privileged EXEC mode

monitor mlt error main

Monitor MultiLink Trunking (MLT) general error information.

Syntax

monitor mlt error main

monitor mlt error main <1–512>

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.

Default

None

Command mode

Privileged EXEC mode

show ist mlt

Displays MultiLink Trunking (MLT) interswitch Trunk (IST) information.

Syntax

show ist mlt

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ist stat

Show IST message statistics.

Syntax

`show ist stat`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show lacp

View LACP configuration information to determine the LACP parameters and to ensure your configuration is correct.

Syntax

`show lacp`

Parameters

Variable	Value
actor-admin interface [gigabitethernet] [vid*<1–4084>] {slot/port[-slot/port][,...]}*	Shows LACP actor administrative information for all interfaces or the specified interface. • **`<1–4084>`** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. • **`{slot/port[-slot/port][,...]}`** is the slot and port list.
actor-oper interface [gigabitethernet] [vid *<1–4084>] {slot/port[-slot/port][,...]}*	Shows LACP actor operational information for all interfaces or the specified interface. • **`<1–4084>`** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. • **`{slot/port[-slot/port][,...]}`** is the slot and port list.
extension interface [gigabitethernet] [vid *<1–4084>] {slot/port[-slot/port][,...]}*	Shows LACP timer information for all interfaces or the specified interface.

Variable	Value
	• **<1–4084>** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. • **{slot/port[-slot/port][,...]}** is the slot and port list.
interface [gigabitethernet] [vid *<1–4084>] {slot/port[-slot/port][,...]}*	Shows all LACP port configuration information for all interfaces or the specified interface.
interface mlt *[<64–6399>]*	Shows the MLT LACP information for all MLTs or the specific MLT index.
partner-admin interface [gigabitethernet] [vid*<1–4084>] {slot/port[-slot/port][,...]}*	Shows LACP partner administrative information for all interfaces or the specified interface. • **<1–4084>** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. • **{slot/port[-slot/port][,...]}** is the slot and port list.
partner-oper interface [gigabitethernet] [vid*<1–4084>] {slot/port[-slot/port][,...]}*	Shows LACP partner operational information for all interfaces or the specified interface. • **<1–4084>** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN. • **{slot/port[-slot/port][,...]}** is the slot and port list.

Default

None

Command mode

Privileged EXEC mode

show mlt

Display MultiLink Trunking (MLT) information, including port type, port members and designated ports.

Syntax

show mlt <1–512>

Parameters

Variable	Value
<1–512>	Specifies the MLT ID. The value ranges from 1–512.

Default

None

Command mode

Privileged EXEC mode

show mlt error collision

View information about collision errors to obtain information about collision errors in the specified MLT, or for all MLTs.

Syntax

`show mlt error collision [<1–512>]`

Parameters

Variable	Value
<1–512>	Specifies the MLT ID. The value ranges from 1–512.

Default

None

Command mode

Privileged EXEC mode

show mlt error main

View information about Ethernet errors to display information about the types of Ethernet errors sent and received by the specified MLT or all MLTs.

Syntax

`show mlt error main [<1–512>]`

Parameters

Variable	Value
<1–512>	Specifies the MLT ID. The value ranges from 1–512.

Default

None

Command mode

Privileged EXEC mode

show smlt

View all ports for a single port SMLT to ensure the correct ports are configured.

Syntax

`show smlt mlt`

Parameters

Variable	Value
`mlt`	Displays SMLT information for the MLT interface.

Default

None

Command mode

Privileged EXEC mode

show vlacp interface

Displays Virtual Link Aggregation Control Protocol (VLACP) global information.

Syntax

`show vlacp`

`show vlacp interface`

`show vlacp interface gigabitethernet {slot/port[-slot/port][,...]}`

show vlacp interface [vid <1–4084>]

Parameters

Variable	Value
vid *<1–4084>*	**<1–4084>** is the VLAN ID or list of VLAN IDs to show only ports attached to a particular VLAN.
gigabitethernet	Displays the VLACP configuration for the GigabitEthernet port interface.
interface	Displays the VLACP port configuration to show the port VLACP configuration.
{slot/port [-slot/port][,...]}	**{slot/port [-slot/port] [,...]}** is the slot and port list.

Default

None

Command mode

Privileged EXEC mode

smlt

Create a SMLT from an existing MLT to split physical ports between two switches to improve resiliency and provide active load sharing.

Syntax

smlt

default smlt

no smlt

Parameters

None

Default

None

Command mode

MLT Interface Configuration mode

vlacp

Configure VLACP on a port to ensure there is end-to-end reachability.

Syntax

`vlacp`

Parameters

Variable	Value
enable	Enables VLACP for this port.
ethertype <*0X600–0Xffff*>	Sets the VLACP protocol identification for this port.
fast-periodic-time <*100-20000*>	Sets the fast periodic time (in milliseconds) for this port.
funcmac-addr <*0x00:0x00:0x00:0x00:0x00:0x00*>	Sets the multicast MAC address used for the VLACPDU. Specify a MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00.
slow-periodic-time <*10000-30000*>	Sets the slow periodic time (in milliseconds) for a specific port type.
timeout {long|short}	Sets the port to use the long or short timeout: • **`long`** sets the port to use the timeout-scale value multiplied by the slow-periodic-time. • **`short`** sets the port to use the timeout-scale value multiplied by the fast-periodic-time. For example, if you specify a short timeout, set the timeout-scale value to 3, and the fast-periodic-time to 400 ms, the timer will expire within 1000 to 1200 ms. To set this option to the default value, use the **`default`** operator with the command.
timeout-scale <*2-10*>	Sets a timeout scale for this port used to calculate the timeout. The default value is 3. To set this option to the default value, use the **`default`** operator with the command.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

vlacp enable

Enable or disable the VLACP globally to reset all port level settings on the chassis.

Syntax

vlacp enable

no vlacp enable

default vlacp enable

Parameters

Variable	Value
enable	Enables the VLACP globallly.

Default

None

Command mode

Global Configuration mode

Chapter 12: OSPF and RIP commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to help you configure the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) on the Avaya Virtual Services Platform 9000. The router uses these protocols to determine the best routes for data forwarding.

accept adv-rtr (for OSPF)

Use a route policy to define how the switch redistributes external routes from a specified source into an OSPF domain. The policy defines which route types the switch accepts and redistributes.

Syntax

accept adv-rtr {A.B.C.D} [enable] [metric-type <type1|type2|any>] [route-policy WORD<0–64>]

default accept adv-rtr {A.B.C.D} [enable] [metric-type] [route-policy]

no accept adv-rtr {A.B.C.D} [enable]

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address.
enable	Enables an OSPF accept entry for a specified advertising router.
metric-type <*type1*|*type2*|*any*>	Indicates the OSPF external type. This parameter describes which types of OSPF external routes match this entry. • any means match all external routes. • type1 means match external type 1 only. • type2 means match external type 2 only.
route-policy *WORD<0-64>*	Specifies the name of the route policy to use for filtering external routes advertised by the specified advertising router before accepting into the routing table.

Default

None

Command mode

OSPF Router Configuration mode

action triggerRipUpdate

Force RIP to update the routing table so that the port or VLAN uses the latest routing information.

Syntax

action triggerRipUpdate

Parameters

None

Default

None

Command mode

GigabitEthernet Interface Configuration mode

area

Import information from other areas to learn their OSPF relationships and create normal, stubby, or not-so-stubby areas (NSSA). Place stubby or NSSAs at the edge of an OSPF routing domain.

Syntax

area {A.B.C.D} default-cost <0-16777215>

area {A.B.C.D} import <external|noexternal|nssa>

area {A.B.C.D} import-summaries enable

area {A.B.C.D} [stub]

default area {A.B.C.D} default-cost

default area {A.B.C.D} import-summaries enable

default area {A.B.C.D} [stub]

no area {A.B.C.D} import-summaries enable

no area {A.B.C.D}

Parameters

Variable	Value
default-cost *<0-16777215>*	Stub area default metric for this stub area, which is the cost from 0 to 16 777 215. This is the metric value applied at the indicated type of service.
import <external|noexternal|nssa>	Specifies the type of area: • external—Stub and NSSA (not so stubby area). are both false • noexternal—Configures the area as stub area. • nssa—Configures the area as NSSA.
import-summaries enable	Configures the area support to import summary advertisements into a stub area. This parameter must be used only if the area is a stub area.
stub	Configures the import external option for this area as stub. A stub area has only one exit point (router interface) from the area.

Default

None

Command mode

OSPF Router Configuration mode

area range

Use aggregate area ranges to reduce the number of link-state advertisements that are required within the area. You can also control advertisements.

Syntax

area range <A.B.C.D> <A.B.C.D/X> <summary-link|nssa-extlink>

Parameters

Variable	Value
<A.B.C.D> <A.B.C.D/X>	**<A.B.C.D>** identifies an OSPF area and **<A.B.C.DX>** is the IP address and subnet mask of the range, respectively.

Variable	Value
<summary-link|nssa-extlink>	Specifies the LSA type. If you configure the range as type nssa-extlink then you cannot configure the advertise-metric.

Default

None

Command mode

OSPF Router Configuration mode

Related commands

Variable	Value
advertise-metric *<0-65535>*	Changes the advertised metric cost of the OSPF area range.
advertise-mode <summarize|suppress|no-summarize>	Changes the advertisement mode of the range.

area virtual-link

Use manual virtual interfaces to provide a backup link for vital OSPF traffic with a minimum of resource use.

Syntax

`area virtual-link <A.B.C.D> <A.B.C.D>`

Parameters

Variable	Value
<A.B.C.D> <A.B.C.D>	Creates a virtual interface area identifier. **`<A.B.C.D> <A.B.C.D>`** specify the area ID and the virtual interface ID, respectively.

Default

None

Command mode

OSPF Router Configuration mode

Related commands

Variable	Value
authentication-key *WORD<0-8>*	Configures the authentication key of up to eight characters.
authentication-type <none|simple|message-digest>	Configures the authentication type for the OSPF area. *auth-type* is none, simple password, or MD5 authentication. If simple, all OSPF updates received by the interface must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key. The default is none.
primary-md5-key <*1-255*>	Changes the primary key used to encrypt outgoing packets. <*1-255*> is the ID for the message digest key.
dead-interval <*0-2147483647*>	Configures the dead interval, in seconds, for the virtual interface, the number of seconds that a router Hello packets are not seen before its neighbors declare the router down. This value must be at least four times the Hello interval value. The default is 60.
hello-interval <*1-65535*>	Configures the Hello interval, in seconds, on the virtual interface for the length of time (in seconds) between the Hello packets that the router sends on the interface. The default is 10.
retransmit-interval <*0-3600*>	Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions. The range is from 0 to 3600.
transit-delay <*0-3600*>	Configures the transit delay for the virtual interface, the estimated number of seconds required to transmit a link-state update over the interface. The range is from 0 to 3600.

area virtual-link message-digest-key

Configure an MD5 key for the virtual interface.

Syntax

area virtual-link message-digest-key <A.B.C.D> <A.B.C.D> <1-255> md5-key WORD<0–16>

Parameters

Variable	Value
<A.B.C.D> <A.B.C.D> <1-255> md5-key WORD<0-16>	Adds an MD5 key to the interface. At most, you can configure two MD5 keys to an interface. • **<A.B.C.D>** identifies an OSPF area. • **<A.B.C.D>** is the virtual interface id. • *<1-255>* is the ID for the message digest key • *WORD<0-16>* is an alphanumeric password in the range of 0 to 16 characters

Default

None

Command mode

OSPF Router Configuration mode

as-boundary-router enable

Configure the router as an autonomous system boundary router (ASBR).

Syntax

as-boundary-router enable

default as-boundary-router [enable]

Parameters

None

Default

The default is disabled.

Command mode

OSPF Router Configuration mode

auto-vlink

Use automatic virtual links to provide an automatic, dynamic backup link for vital OSPF traffic. Automatic virtual links require more system resources than manually configured virtual links.

Syntax

`auto-vlink`

Parameters

None

Default

None

Command mode

OSPF Router Configuration mode

default-metric (for RIP)

Configures RIP default import metric. This value is used by RIP announce of OSPF internal routes if the policy does not specify metric. 0 is used for deconfiguration.

Syntax

`default-metric <0-15>`

`default default-metric`

Parameters

Variable	Value
<0-15>	Configures the value of default import metric to import a route into RIP domain.

Default

The default value is 8.

Command mode

RIP Router Configuration mode

domain

Specifies the RIP domain.

Syntax

`domain <0-39321>`

`default domain`

Parameters

Variable	Value
<0-39321>	Specifies the RIP domain.

Default

The default is 0.

Command mode

RIP Router Configuration mode

host-route

Use host routes when the Virtual Services Platform 9000 resides in a network that uses routing protocols other than OSPF.

Syntax

`host-route <A.B.C.D> [metric <0-65535>]`

Parameters

Variable	Value
`<A.B.C.D>`	Specifies the IP address of the host router in a.b.c.d format.
`metric <0-65535>`	Configures the metric (cost) for the host route.

Default

None

Command mode

OSPF Router Configuration mode

ip ospf area

Configure OSPF parameters on a port or VLAN to control how OSPF behaves on the port or VLAN.

Syntax

`ip ospf area <A.B.C.D>`

Parameters

Variable	Value
`area <A.B.C.D>`	Configures the OSPF identification number for the area, typically formatted as an IP address.

Default

None

Command mode

VLAN Interface Configuration mode

Related commands

Variable	Value
advertise-when-down enable	Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, the route is not advertised until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.
authentication-key *WORD<0-8>*	Configures the eight-character simple password authentication key for the port or VLAN.
authentication-type <none|message-digest|simple>	Configures the OSPF authentication type for the port: none, simple password, or MD5 authentication. If simple, all OSPF updates the interface receives must contain the authentication key specified by the area authentication-key command. If MD5, they must contain the MD5 key.

Variable	Value
cost <*1-65535*>	Configures the OSPF cost associated with this interface and advertised in router link advertisements. The default is 0.
dead-interval <*0-2147483647*>	Configures the router OSPF dead interval—the number of seconds the OSPF neighbors of a switch must wait before assuming that the OSPF router is down. The default is 40. The value must be at least four times the Hello interval.
enable	Enables OSPF on the port or VLAN.
hello-interval <*1-65535*>	Configures the OSPF Hello interval, which is the number of seconds between Hello packets sent on this interface. The default is 10.
message-digest-key <*1-255*> md5-key *WORD*<*0-16*>	Configures the MD5 key. At most, you can configure two MD5 keys for an interface. • <*1-255*> is the ID for the message digest key • *WORD*<*0-16*> is an alphanumeric password of up to 16 bytes {string length 0 to 16}
mtu-ignore enable	Enables MTU ignore. To allow the Virtual Services Platform 9000 to accept OSPF database description (DBD) packets with a different MTU size, enable mtu-ignore. Incoming OSPF DBD packets are dropped if their MTU is greater than 1500 bytes.
network <broadcast|nbma|passive>	Specifies the type of OSPF interface.
poll-interval <*0-2147483647*>	Configures the OSPF poll interval in seconds. The default is 120.
primary-md5-key <*1-255*>	Changes the primary key used to encrypt outgoing packets. <*1-255*> is the ID for the new message digest key.
priority <*0-255*>	Configures the OSPF priority for the port during the election process for the designated router. The port with the highest priority number is the best candidate for the designated router. If you configure the priority to 0, the port cannot become either the designated router or a backup designated router. The default is 1.
retransmit-interval <*0-3600*>	Configures the retransmit interval for the virtual interface, the number of seconds between link-state advertisement retransmissions.
transit-delay <*0-3600*>	Configures the transit delay for the virtual interface, which is the estimated number of seconds required to transmit a link-state update over the interface.
vlan <*1-4084*>	Applies only to VLAN interfaces. Specifies the VLAN ID.

ip ospf apply redistribute

Apply the OSPF redistribution.

Syntax

ip ospf apply redistribute WORD<1–32> [vrf <WORD 0-16>] [vrf-src WORD<0-16>]

Parameters

Variable	Value
WORD<1–32>	Specifies the type of routes to be redistributed (the protocol source), including OSPF, BGP, static, direct and RIP.
vrf *WORD<0-16>*	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
vrf-src *WORD<0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

Privileged EXEC mode

ip ospf redistribute

Configure a redistribute entry to announce certain routes into the RIP domain, including static routes, direct routes, RIP, OSPF, or BGP. Optionally, use a route policy to control the redistribution of routes.

Syntax

ip ospf redistribute <ospf|bgp|static|direct|rip>

ip ospf redistribute WORD <1–32>

Parameters

Variable	Value
<ospf|bgp|static|direct|rip>	Specifies the type of routes to be redistributed (the protocol source).
vrf *WORD <0-16>*	Specifies the VRF instance.
vrf-src *WORD <0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

VRF Router Configuration mode

Related commands

Variable	Value
apply [vrf-src *WORD<0–16>*	Applies the redistribution configuration. Changes do not take effect until you apply them.
enable [vrf-src *WORD<0–16>*	Enables the OSPF route redistribution instance.
metric <metric-value> [vrf-src *WORD<0–16>*	Configures the metric to apply to redistributed routes.
metric-type <type1|type2> [vrf-src *WORD<0–16>*	Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.
route-policy <policy name> [vrf-src *WORD<0–16>*	Configures the route policy to apply to redistributed routes.
subnets <allow|suppress> [vrf-src *WORD<0–16>*	Allows or suppresses external subnet route advertisements when routes are redistributed into an OSPF domain.

ip ospf spf-run

Force the switch to update its shortest-path calculations so that the switch uses the latest OSPF routing information.

Syntax

`ip ospf spf-run [vrf WORD<0-16>]`

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies a VRF instance by name.

Default

None

Command mode

Privileged EXEC mode

ip rip

Configure RIP on Ethernet ports and VLANs so that they can participate in RIP routing.

Syntax

`ip rip cost <1-15>`

Parameters

Variable	Value
cost <*1-15*>	Configures the RIP cost for this port (link).

Default

None

Command mode

VLAN or GigabitEthernet Interface Configuration mode

Related commands

Variable	Value
advertise-when-down enable	Enables or disables AdvertiseWhenDown. If enabled, the network on this interface is advertised as up, even if the port is down. The default is disabled. When you configure a port with no link and enable advertise-when-down, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link status, this parameter must be disabled.

Variable	Value
auto-aggregation enable	Enables or disables automatic route aggregation on the port. When enabled, the router switch automatically aggregates routes to their natural mask when they are advertised on an interface in a different class network. The default is disable.
default-listen enable	Enables DefaultListen: the switch accepts the default route learned through RIP on this interface. The default is disabled.
default-supply enable	Enables DefaultSupply. If enabled, a default route must be advertised from this interface. The default is false. The default route is advertised only if it exists in the routing table.
enable	Enables RIP routing on the port.
holddown *<0-360>*	Configures the RIP holddown timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable. The default is 120.
in-policy *WORD<0-64>*	Configures the port RIP in-policy. The policy name for inbound filtering on this RIP interface. This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.
listen enable	If enabled, the switch listens for a default route without listening for all routes. Specifies that the routing switch learns RIP routes through this interface. The default is enable.
out-policy *WORD<0-64>*	Configures the port RIP out-policy. The policy name for outbound filtering on this RIP interface. This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. *policy name* is a string of length 0 to 64 characters.
poison enable	Enables Poison Reverse. If you disable Poison Reverse (**`no poison enable`**), Split Horizon is enabled. By default, Split Horizon is enabled. If Split Horizon is enabled, IP routes learned from an immediate neighbor are not advertised back to the neighbor. If Poison Reverse is enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. These mechanisms prevent routing loops.
send version <notsend|rip1| rip1comp|rip2>	Indicates which RIP update version the router sends from this interface. ripVersion1 implies sending RIP updates that comply with RFC 1058. rip1Compatible implies

Variable	Value
	broadcasting RIP2 updates using RFC 1058 route subassumption rules. The default is rip1Compatible.
receive version <rip1|rip2|rip1orrip2>	Indicates which RIP update version is accepted on this interface. The default is rip1orrip2.
supply enable	Specifies that the switch advertises RIP routes through the port. The default is enable.
timeout <*15-259200*>	Configures the RIP timeout interval in seconds.
triggered enable	Enables automatic triggered updates for RIP.

ip rip apply redistribute

Apply the RIP redistribution.

Syntax

ip rip apply redistribute WORD<0–32> [vrf WORD<0-16>] [vrf-src WORD<0-16>]

Parameters

Variable	Value
WORD<0–32>	Specifies the type of routes to be redistributed (the protocol source), including OSPF, BGP, static, direct, RIP.
vrf *WORD<0-16>*	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
vrf-src *WORD<0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

Privileged EXEC mode

ip rip redistribute

Configure a redistribute entry to announce certain routes into the RIP domain, including static routes, direct routes, RIP, OSPF, or BGP. Optionally, use a route policy to control the redistribution of routes.

Syntax

`ip rip redistribute <ospf|bgp|static|direct|rip>`

Parameters

Variable	Value
<ospf|bgp|static|direct|rip>	Specifies the type of routes to be redistributed (the protocol source).
vrf *WORD <0-16>*	Specifies the VRF instance.
vrf-src *WORD <0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

VRF Router Configuration mode

Related commands

Variable	Value
enable [vrf-src *WORD<0-16>]*	Enables the RIP route redistribution instance.
metric *<0-255>* [vrf-src *WORD <0-16>]*	Configures the metric to apply to redistributed routes.
route-map *WORD <0-64>* [vrf-src *WORD <0-16>]*	Configures the route policy to apply to redistributed routes.

neighbor (for OSPF)

Configure NBMA neighbors so that the interface can participate in Designated Router election. All OSPF neighbors that you manually configure are NBMA neighbors.

Syntax

neighbor {A.B.C.D} [priority <0-255>]

default neighbor {A.B.C.D}

no neighbor {A.B.C.D}

Parameters

Variable	Value
<A.B.C.D>	Identifies an OSPF area in IP address format A.B.C.D.
priority *<0-255>*	Changes the priority level of the neighbor.

Default

None

Command mode

OSPF Router Configuration mode

network (for RIP)

Enables RIP on a network.

Syntax

network {A.B.C.D}

no network {A.B.C.D}

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address of the network.

Default

None

Command mode

RIP Router Configuration mode

redistribute (for RIP)

Configure a redistribute entry to announce certain routes into the RIP domain, including static routes, direct routes, RIP, OSPF, or BGP. Optionally, use a route policy to control the redistribution of routes.

Syntax

redistribute WORD<0-32> enable vrf-src WORD<0-16>

redistribute WORD<0-32> enable

redistribute WORD<0-32> metric <0-65535> vrf-src WORD<0-16>

redistribute WORD<0-32> metric <0-65535>

redistribute WORD<0-32> route-map WORD<0-64> vrf-src WORD<0-16>

redistribute WORD<0-32> route-map WORD<0-64>

redistribute WORD<0-32> vrf-src WORD<0-16>

redistribute WORD<0-32>

default redistribute WORD<0-32> enable vrf-src WORD<0-16>

default redistribute WORD<0-32> enable

default redistribute WORD<0-32> metric vrf-src WORD<0-16>

default redistribute WORD<0-32> metric

default redistribute WORD<0-32> route-map vrf-src WORD<0-16>

default redistribute WORD<0-32> route-map

default redistribute WORD<0-32> vrf-src WORD<0-16>

default redistribute WORD<0-32>

no redistribute WORD<0-32> enable vrf-src WORD<0-16>

no redistribute WORD<0-32> enable

no redistribute WORD<0-32> route-map vrf-src WORD<0-16>

no redistribute WORD<0-32> route-map

no redistribute WORD<0-32> vrf-src WORD<0-16>

no redistribute WORD<0-32>

Parameters

Variable	Value
<0-65535>	Configures the metric to apply to redistributed routes
vrf-src *WORD<0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.
WORD<0-32>	Specifies the type of routes to be redistributed (the protocol source). Options are {bgp|direct|ospf|rip|static}
WORD<0-64>	Configures the route policy to apply to redistributed routes.

Default

None

Command mode

RIP Router Configuration mode

redistribute (for OSPF)

Configure a redistribute entry to announce certain routes into OSPF, including static routes, direct routes, RIP, OSPF, or BGP. Optionally, use a route policy to control the redistribution of routes.

Syntax

`redistribute <ospf|bgp|static|direct|rip> [vrf-src WORD<0-16>]`

Parameters

Variable	Value
<ospf|bgp|static|direct|rip>	Specifies the type of routes to be redistributed (the protocol source).
vrf-src *WORD<0-16>*	Specifies the source VRF instance. This parameter is not required for redistribution within the same VRF.

Default

None

Command mode

OSPF Router Configuration mode

Related commands

Variable	Value
enable [vrf-src *WORD<0-16>]*	Enables the OSPF route redistribution instance.
metric *<0–65535>* [vrf-src *<WORD 0-16>]*	Configures the metric to apply to redistributed routes.
metric-type <type1|type2> [vrf-src *WORD<0-16>]*	Specifies a type 1 or a type 2 metric. For metric type 1, the cost of the external routes is equal to the sum of all internal costs and the external cost. For metric type 2, the cost of the external routes is equal to the external cost alone.
route-policy *WORD<0-64>* [vrf-src *WORD<0-16>]*	Configures the route policy to apply to redistributed routes.
subnets <allow|suppress> [vrf-src *WORD<0-16>]*	Allows or suppresses external subnet route advertisements when routes are redistributed into an OSPF domain.

router ospf

Enable OSPF for the switch. If you do not use an optional parameter with the command, you enter the OSPF Router Configuration mode.

Syntax

`router ospf [enable|ipv6-enable]`

`default router ospf [enable|ipv6-enable]`

`no router ospf [enable|ipv6-enable]`

Parameters

Variable	Value
enable	Enables OSPF routing on the Virtual Services Platform 9000.
ipv6-enable	Enables OSPFv3 for IPv6 routing.

Default

None

Command mode

Global Configuration mode

router rip enable

Enable RIP globally.

Syntax

`router rip enable vrf <1–511>`

Parameters

Variable	Value
enable	Globally enables RIP on the VRF or switch.
vrf <*1–511*>	Enables rip for a particular VRF. <*1–511*> denotes the range of the VRF id.

Default

None

Command mode

Global Configuration mode

router-id (for OSPF)

Configure OSPF parameters on the switch to control how OSPF behaves on the system. The Virtual Services Platform 9000 uses global parameters to communicate with other OSPF routers. Globally configure OSPF before you configure OSPF for an interface, port, or VLAN.

Syntax

`router-id <A.B.C.D>`

Parameters

Variable	Value
router-id <*A.B.C.D*>	Configures the OSPF router ID IP address, where A.B.C.D is the IP address.

Default

None

Command mode

OSPF Router Configuration mode

show ip ospf

Display OSPF configuration information to ensure accuracy.

Syntax

show ip ospf [vrf WORD <0-16>] [vrfids WORD <0-512>]

Parameters

Variable	Value
vrf *WORD <0-16>*	Specifies a VRF by name.
vrfids *WORD <0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf accept

Display information about the configured OSPF entries.

Syntax

show ip ospf accept [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	The name of the VRF.
vrf ids *WORD<0-512>*	The ID of the VRF. The value is an integer between 0 and 512.

Default

None

Command mode

Privileged EXEC mode

show ip ospf area

Display OSPF area information to ensure accuracy.

Syntax

`show ip ospf area [vrf WORD<0-16>] [vrfids WORD<0-512>]`

Parameters

Variable	Value
vrf *WORD <0-16>*	Specifies a VRF by name.
vrfids *WORD <0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf area-range

Display OSPF area range configuration information to ensure accuracy.

Syntax

`show ip ospf area-range [vrf <WORD 0-16>] [vrfids <WORD 0-512>]`

Parameters

Variable	Value
vrf <*WORD 0-16*>	Specifies a VRF by name.
vrfids <*WORD 0-512*>	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf ase

View the link-state database to determine externally learned routing information.

Syntax

show ip ospf ase [metric-type <1-2>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
metric-type *<1-2>*	Specifies the metric type as a string of 1 to 2 characters.
vrf *WORD<0-16>*	Identifies the VRF by name.
vrfids *WORD<0-512>*	Specifies a VRF by ID.

Default

None

Command mode

Privileged EXEC mode

show ip ospf authentication

Display OSPF authentication information to ensure accuracy.

Syntax

show ip ospf authentication interface [gigabitethernet {slot/port}| vlan <1–4084>]

Parameters

Variable	Value
gigabitethernet *{slot/port}* vlan *<1–4084>*	Specifies the authentication interface type.

Default

None

Command mode

Privileged EXEC mode

show ip ospf default-cost

Display OSPF default cost information to ensure accuracy.

Syntax

show ip ospf default-cost [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf WORD<0-16>	Specifies a VRF by name.
vrfids WORD<0-512>	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf host-route

Display the host route OSPF information to ensure accuracy.

Syntax

show ip ospf host-route [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf int-auth

Display OSPF authentication information to ensure accuracy.

Syntax

show ip ospf int-auth [vrf WORD <0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf WORD<0-16>	Displays ospf authentication configuration for a particular VRF.
vrfids WORD<0-512>	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf interface

Display OSPF information on a particular interface to ensure accuracy.

Syntax

show ip ospf interface [gigabitethernet {slot/port}|vlan <1–4084>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
gigabitethernet *{slot/[port]}* |vlan *<1–4084>*	Displays gigabitethernets port and vlan ids information.

Variable	Value
vrf *WORD<0-16>*	Displays ospf configuration for a particular VRF.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf int-timers

Display OSPF timers information to ensure accuracy.

Syntax

show ip ospf int-timers [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	Displays ospf timer configuration for a particular VRF.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf lsdb

View the area advertisements and other information contained in the link-state database (LSD) to ensure correct OSPF operations.

Syntax

show ip ospf lsdb [area <A.B.C.D>] [lsa-type <0-7>] [lsid <A.B.C.D>] [adv-rtr <A.B.C.D>] [vrf WORD<0-16>] [vrfids WORD<0-512>] [detail]

Parameters

Variable	Value
adv-rtr *<A.B.C.D>*	Specifies the advertising router.
area *<A.B.C.D>*	Specifies the OSPF area.
detail	Provides detailed output.
lsa-type *<0-7>*	Specifies the link-state advertisement type in the range of 0 to 7.
lsid *<A.B.C.D>*	Specifies the link-state ID.
vrf *WORD<0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf neighbor

Display OSPF NBMA neighbor information.

Syntax

show ip ospf neighbor [vrf WORD<0-16>] [vrfids WORD <0-512>]

Parameters

Variable	Value
vrf *WORD <0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf port-error

Check OSPF errors for administrative and troubleshooting purposes.

Syntax

show ip ospf port-error [port <portList>] [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
port *{slot/port [-slot/port][,...]}*	Specifies the slot and the port number.
vrf *WORD<0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf redistribute

Display the OSPF redistribution configuration information.

Syntax

show ip ospf redistribute [vrf WORD <0-16>] [vrfids WORD<1-512>]

Parameters

Variable	Value
vrf *WORD <0-16>*	Specifies a VRF by name.
vrfids *WORD <0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip ospf virtual-link

Display the OSPF virtual link information to ensure accuracy.

Syntax

show ip ospf virtual-link {A.B.C.D} {A.B.C.D} [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
{A.B.C.D} {A.B.C.D}	Specifies the area ID and the virtual interface ID. The first IP address specifies the area ID and the second specifies the virtual interface ID.
vrf *WORD<0-16>*	Displays OSPF configuration for a particular VRF. Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip rip

Display RIP configuration information to ensure the configuration is accurate.

Syntax

show ip rip [vrf WORD<0-16>] [vrfids WORD<0-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies a VRF by name.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip rip interface

Displays Routing Information Protocol (RIP) information for each interface.

Syntax

show ip rip interface ports [{slot/port [-slot/port][,...]}]

show ip rip interface vlan [<1–2084>]

show ip rip interface {A.B.C.D}

show ip rip interface [vrf WORD<0-16>] [vrfids WORD<1-512>]

Parameters

Variable	Value
{A.B.C.D}	SHows configurations based on an IP address assigned to a VLAN.
ports *{slot/port [-slot/port][,...]}*	Shows RIP information for port configurations. *{slot/port [-slot/port][,...]}* specifies the port.
vlan <*1–4084*>	Shows RIP configuration information for a particular VLAN. <*1–4084*> specifies the VLAN ID.
vrf *WORD<0-16>*	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show ip rip redistribute

Display the RIP redistribution configuration information.

Syntax

show ip rip redistribute [vrf WORD<0-16>] [vrfids WORD<1-512>]

Parameters

Variable	Value
vrf *WORD<0-16>*	Specifies the VRF instance by name. When applying a redistribution instance that redistributes from a nonzero VRF to VRF 0 (the global router), do not specify the destination VRF; only specify the source VRF.
vrfids *WORD<0-512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

timers basic holddown

Configures the RIP hold-down timer value, the length of time (in seconds) that RIP continues to advertise a network after determining that it is unreachable.

Syntax

timers basic holddown <0-360>

default timers basic holddown

Parameters

Variable	Value
<0-360>	Configures the timer value.

Default

The default is 120 seconds.

Command mode

RIP Router and OSPF Router Configuration mode

timers basic timeout

Configures the RIP timeout interval.

Syntax

timers basic timeout <15-259200>

default timers basic timeout

Parameters

Variable	Value
<15-259200>	Configures the value of default import metric to import a route into RIP domain.

Default

The default value is 180.

Command mode

RIP Router Configuration mode

timers basic update

Configures the RIP update timer. The update time is the time interval between RIP updates.

Syntax

timers basic update <1-360>

default timers basic update

Parameters

Variable	Value
<1-360>	Configures the update interval.

Default

The default is 30 seconds.

Command mode

RIP Router Configuration mode

Chapter 13: Performance management commands

This chapter describes Avaya Command Line Interface (ACLI) commands about switch management tools, the Simple Network Management Protocol (SNMP), RMON, and configuration of the Web management interface for the Avaya Virtual Services Platform 9000.

clear-stats

Clear port statistic counters.

Syntax

clear-stats [port {slot/port[-slot/port][,...]}

Parameters

Variable	Value
{slot/port[-slot/port][,...]	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

clear alarm

Clear the alarm database to remove old information after a condition is resolved or to reset statistics.

Syntax

clear alarm database

clear alarm database alarm-id WORD<0-100>

clear alarm statistics

Parameters

Variable	Value
database	Clears the alarm database.
statistics	Clears the alarm database statistics.
WORD<0–100>	Specifies an alarm ID to clear.

Default

None

Command mode

Privileged EXEC mode

clear filter acl

Clear ACL statistics if you no longer require previous statistics or log information.

Syntax

clear filter acl log

clear filter acl statistics all

clear filter acl statistics default <1-2048>

clear filter acl statistics default

clear filter acl statistics global

clear filter acl statistics global <1-2048>

clear filter acl statistics <1-2048> <1-2000>

clear filter acl statistics <1-2048> qos

clear filter acl statistics <1-2048> security

clear filter acl statistics <1-2048>

Parameters

Variable	Value
[<1-2048>]	Specifies the ACL identifier.

Variable	Value
<1–2000>	Specifies the ACE identifier.
qos	Clears ACL statistics for QoS ACEs.
security	Clears ACL statistics for Security ACEs.
all	Clear all statistics for all access control entries.
default *<1–2048>*	Clear traffic statistics for an access control entry.
global *<1–2048>*	Clear global statistics for an access control entry.

Default

None

Command mode

Privileged EXEC mode

clear ip ipfix hash-stats

Clear IPFIX statistics to remove the hash statistics.

Syntax

`clear ip ipfix hash-stats [{slot[-slot][,...]}]`

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). If you do not specify a slot, you clear the statistics for all slots. Valid slots are 3–12.

Default

None

Command mode

Privileged EXEC mode

clear ip ipfix stats

Clear IPFIX statistics to remove the exporter statistics.

Syntax

clear ip ipfix stats [{slot[-slot][,...]}]

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). If you do not specify a slot, you clear the statistics for all slots. Valid slots are 3–12.

Default

None

Command mode

Privileged EXEC mode

clear ip mroute stats

Clear multicast routing process statistics.

Syntax

clear ip mroute stats

Parameters

None

Default

None

Command mode

Privileged EXEC mode

clear ipv6 statistics interface

Use this command to clear IPv6 statistics.

Syntax

clear ipv6 statistics all

clear ipv6 statistics interface

clear ipv6 statistics interface [general|icmp] [gigabitEthernet {slot/port}|mgmtethernet {slot/port}|tunnel<1–2000>|vlan <1–4084>]

clear ipv6 statistics tcp

clear ipv6 statistics udp

Parameters

Variable	Value
all	Clears all statistics.
general	Clears general statistics.
gigabitEthernet*{slot/port}*	Clears statistics for a brouter interface.
icmp	Clears Internet Control Message Protocol (ICMP) statistics.
mgmtethernet*{slot/port}*	Clears statistics for a management port.
tunnel *<1–2000>*	Clears statistics for a tunnel
vlan *<1–4084>*	Clears statistics for a tunnel.
tcp	Clears TCP statistics.
udp	Clears UDP statistics.

Default

None

Command mode

Privileged EXEC mode

clear lacp

Clear link aggregation information and statistics.

Syntax

clear lacp link-aggregate <1–512>

clear lacp stats [port {slot/port[-slot/port][,...]}]

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

clear logging

Clear the log file.

Syntax

clear logging

Parameters

None

Default

None

Command mode

Privileged EXEC mode

clear mac-address-table

Clear the entries in the MAC address table.

Syntax

clear mac-address-table port {slot/port[-slot/port][,...]} address WORD<17–17>

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
WORD<17—17>	Specifies the MAC address.

Default

None

Command mode

Privileged EXEC mode

clear mlt

Clear IST statistics.

Syntax

clear mlt ist stats

Parameters

None

Default

None

Command mode

Privileged EXEC mode

clear qos

Clear quality of service (QoS) information.

Syntax

clear qos statistics policy [<1–16000>] [slot {slot[-slot][,...]}]

Parameters

Variable	Value
<1–16000>	Specifies a policy ID.
slot {slot[-slot][,...]}	Clears QoS statistics for a specific slot, from 3–12.

Default

None

Command mode

Privileged EXEC mode

clear radius statistics

Clear server statistics.

Syntax

clear radius statistics

Parameters

None

Default

None

Command mode

Privileged EXEC mode

clear telnet

Close open Telnet sessions.

Syntax

clear telnet <0–7>

Parameters

Variable	Value
<0–7>	Specifies the Telnet session ID to close.

Default

None

Command mode

Privileged EXEC mode

clear trace

Clear the trace file.

Syntax

clear trace

Parameters

None

Default

None

Command mode

Privileged EXEC mode

ip ipfix (on a port)

Configure IPFIX on a port to meter IP flows on the port.

Syntax

ip ipfix [port {slot/port[-slot/port][,...]}] sampling-rate <1–100000>

ip ipfix [port {slot/port[-slot/port][,...]}] enable

default ip ipfix [port {slot/port[-slot/port][,...]}] sampling-rate

default ip ipfix [port {slot/port[-slot/port][,...]}] enable

no ip ipfix [port {slot/port[-slot/port][,...]}]

no ip ipfix [port {slot/port[-slot/port][,...]}] enable

Parameters

Variable	Value
sampling-rate *<1–100000>*	Configures the sampling rate for metering on the port, as one in every n packets. The default value is 1, which configures continuous monitoring.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
enable	Enables IPFIX on the port.

Default

The default sampling rate is 1.

Command mode

GigabitEthernet Interface Configuration mode

ip ipfix enable

Enable IPFIX to use IPFIX in filters or on a port.

Syntax

`ip ipfix enable`

`default ip ipfix enable`

`no ip ipfix enable`

Parameters

Variable	Value
enable	Enables IPFIX globally.

Default

The default is disabled.

Command mode

Global Configuration mode

ip ipfix collector

Configure collector parameters to determine to which collector a slot exports flow information. You can configure up to two collectors for each slot.

Specify an exporter IP address to configure the source address in the IPFIX packets the interface module sends to the collectors. If you do not specify an exporter IP address, the source IP address is chosen from virtual IP, management IP, or outgoing interface IP based on the collector IP reachability.

Syntax

ip ipfix collector {slot[-slot][,...]} {A.B.C.D} dest-port <1-65535> [exporter-ip {A.B.C.D}]

ip ipfix collector {slot[-slot][,...]} {A.B.C.D} protocol udp

ip ipfix collector {slot[-slot][,...]} {A.B.C.D} enable

default ip ipfix collector {slot[-slot][,...]} {A.B.C.D} dest-port [exporter-ip]

default ip ipfix collector {slot[-slot][,...]} {A.B.C.D} enable [protocol]

no ip ipfix collector {slot[-slot][,...]} {A.B.C.D} enable

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address of the collector.
dest-port <*1-65535*>	Specifies the destination port.
exporter-ip {A.B.C.D}	Specifies the IP address for the exported traffic.
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).
enable	Enables the collector status.
protocol udp	Specifies the protocol.

Default

None

Command mode

Global Configuration mode

ip ipfix flush

Flush IPFIX flow information to delete all records that correspond to the port number you specify.

Syntax

ip ipfix flush port {slot/port[-slot/port][,...]} [export-and-flush]

Parameters

Variable	Value
export-and-flush	Optionally, initiates an export of all records, and then deletes the database after the export finishes. in UDP-based transport, the exporter sends out the flow database once, but there is no guarantee that the export reaches the collector. In TCP/SCTP-based transport, the receipt of the export by the collector is guaranteed.
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).

Default

None

Command mode

Privileged EXEC mode

ip ipfix slot

Configure IPFIX on an interface module to specify active flow parameters.

Syntax

ip ipfix slot {slot[-slot][,...]} active-timeout <1–60>

ip ipfix slot {slot[-slot][,...]} aging-interval <10-3600>

ip ipfix slot {slot[-slot][,...]} export-interval <10-3600>

ip ipfix slot {slot[-slot][,...]} exporter-enable

ip ipfix slot {slot[-slot][,...]} template-refresh-interval <60–3600>

ip ipfix slot {slot[-slot][,...]} template-refresh-packets <1–600>

default ip ipfix slot {slot[-slot][,...]} active-timeout

default ip ipfix slot {slot[-slot][,...]} aging-interval

default ip ipfix slot {slot[-slot][,...]} export-interval

default ip ipfix slot {slot[-slot][,...]} exporter-enable

default ip ipfix slot {slot[-slot][,...]} template-refresh-interval

default ip ipfix slot {slot[-slot][,...]} template-refresh-packets

no ip ipfix slot {slot[-slot][,...]}

no ip ipfix slot {slot[-slot][,...]} exporter-enable

Parameters

Variable	Value
active-timeout <*1–60*>	Configures the flow active timeout.
aging-interval <*10-3600*>	Configures the flow record aging interval.
export-interval <*10-3600*>	Configure the interval at which to export flow information.
exporter-enable	Enables the exporter state for the slot.
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3–4), or a series of slots (3,5,6). Valid slots are 3–12.
template-refresh-interval <*60–3600*>	Configures the template refresh timeout. The template is sent to the collector every x seconds or after x exported packets, whichever occurs first.
template-refresh-packets <*1–600*>	Configures the template refresh timeout. The template is sent to the collector every x seconds or after x exported packets, whichever occurs first. .

Default

The following list identifies the default values:

- active-timeout: 30 minutes
- aging-interval: 15 seconds
- export-interval: 50 seconds
- exporter-enable: enable

- template-refresh-interval: 60 seconds
- template-refresh-packets: 20 packets

Command mode

Global Configuration mode

ip mroute stats enable

Enable the collection of multicast routing process statistics.

Syntax

ip mroute stats enable

default ip mroute stats enable

no ip mroute stats enable

Parameters

None

Default

The default is disabled.

Command mode

Global Configuration mode

mac-security mac-da-filter

Add or delete a global MAC filter for MAC security.

Syntax

mac-security mac-da-filter [add|delete]

Parameters

Variable	Value
add *{0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00}*	Adds a global filter. *{0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00}* specifies the MAC address to be added.
delete *0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00}*	Deletes a global filter. *{0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00}* specifies the MAC address to be deleted.

Default

None

Command mode

Global Configuration mode

monitor ip mroute stats

Display multicast routing process statistics at regular intervals.

Syntax

monitor ip mroute stats WORD<7-160>

Parameters

Variable	Value
WORD<7-160>	Specifies the group IP address in the format {A.B.C.D[,E.F.G.H][,...]} . The maximum number of group IP addresses is 10. To view statistics, the group IP address is optional. To monitor statistics, the group IP address is required.

Default

None

Command mode

Privileged EXEC mode. You can change the duration or interval for monitoring in the Global Configuration mode.

monitor ip vrrp statistics

Display IP multicast statistics for the Virtual Router Redundancy Protocol (VRRP).

Syntax

monitor ip vrrp statistics gigabitethernet

monitor ip vrrp statistics gigabitethernet verbose

monitor ip vrrp statistics gigabitethernet {slot/port [-slot/port] [,...]}

monitor ip vrrp statistics gigabitethernet {slot/port [-slot/port] [,...]} verbose

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port] [,...]}*	Specifies the slot and port.
verbose	Specifies the complete list of configuration information.

Default

None

Command mode

Privileged EXEC mode

monitor mlt stats interface main

Show MultiLink Trunking (MLT) interface statistics.

Syntax

monitor mlt stats interface main

monitor mlt stats interface main<1–512>

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.

Default

None

Command mode

Privileged EXEC mode

monitor mlt stats interface utilization

Show MultiLink Trunking (MLT) interface statistics utilization.

Syntax

monitor mlt stats interface utilization

monitor mlt stats interface utilization <1–512>

Parameters

Variable	Value
<1–512>	Specifies the MLT ID.

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics bridging

Monitor port bridging statistics.

Syntax

monitor ports statistics bridging

monitor ports statistics bridging from {slot/port [-slot/port][,...]}

Parameters

Variable	Value
bridging	Monitor port bridging statistics.
bridging from*{slot/port [-slot/port][,...]}*	Monitor port bridging statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics dhcp-relay

Monitor port dhcp-relay statistics.

Syntax

monitor ports statistics dhcp-relay

monitor ports statistics dhcp-relay from {slot/port [-slot/port] [,...]}

Parameters

Variable	Value
dhcp-relay	Monitor port DHCP-relay statistics.
dhcp-relay from*{slot/port [-slot/port][,...]}*	Monitor port DHCP-relay statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics interface

Monitor port interface statistics.

Syntax

monitor ports statistics interface main

monitor ports statistics interface main from {slot/port [-slot/port] [,...]}

monitor ports statistics interface utilization

monitor ports statistics interface utilization from {slot/port [-slot/port][,...]}

monitor ports statistics interface verbose

monitor ports statistics interface verbose from {slot/port [-slot/port][,...]}

Parameters

Variable	Value
main	Monitor port interface statistics.
main from *{slot/port [-slot/port][,...]}*	Monitor port interface statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
utilization	Monitor port interface utilization statistics.
utilization from*{slot/port [-slot/port][,...]}*	Monitor port interface utilization statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
verbose	Monitor port interface statistics.
verbose *{slot/port [-slot/port][,...]}*	Monitor port interface statistics from a particular starting port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
{slot/port [-slot/port][,...]}	Specifies the slot and port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics ospf main

Monitor ports statistics for open shortest path first (OSPF) performance.

Syntax

monitor ports statistics ospf main

monitor ports statistics ospf main from {slot/port[-slot/port][,...]}

monitor ports statistics ospf verbose

monitor ports statistics ospf verbose from {slot/port[-slot/port][,...]}

Parameters

Variable	Value
main	Monitor ports statistics for OSPF main command.
main from *{slot/port[-slot/port][,...]}*	Monitor ports statistics for OSPF main command from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
verbose	Monitor ports statistics for OSPF verbose command.
verbose from *{slot/port[-slot/port][,...]}*	Monitor ports statistics for OSPF verbose command. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics rmon

Monitor port remote monitoring (RMON) statistics.

Syntax

monitor ports statistics rmon

monitor ports statistics rmon from {slot/port[-slot/port][,...]}

Parameters

Variable	Value
rmon	Monitors port remote monitoring statistics.
rmon *{slot/port[-slot/port][,...]}*	Monitors port remote monitoring statistics from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

monitor ports statistics routing

Monitor port Dynamic Host Configuration Protocol (DHCP) routing statistics.

Syntax

`monitor ports statistics routing`

`monitor ports statistics routing from {slot/port[-slot/port][,...]}`

Parameters

Variable	Value
routing	Monitors port DHCP routing statistics.
routing from *{slot/port[-slot/port][,...]}*	Monitors port DHCP routing statistics from a particular port. Identifies the slot and port in one of the following formats: a single slot and port (3/1),a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

pluggable-optical-module

Configure Digital Diagnostic Interface (DDI) on Digital Diagnostic Monitoring to get information concerning the status of the transmitted and received signals to allow better fault isolation and error detection.

Syntax

`pluggable-optical-module ddm-alarm-portdown`

Parameters

Variable	Value
ddm-alarm-portdown	Sets the port down when an alarm occurs. When enabled, the port goes down when any alarm occurs.

Default

The default is disable.

Command mode

Global Configuration mode

Related commands

Variable	Value
ddm-monitor	Enables the monitoring of the DDM. When enabled, the user gets the internal performance condition (temperature, voltage, bias, Tx power and Rx power) of the SFP/XFP. The default is disable.
ddm-monitor-interval <*5-60*>	Configures the DDM monitor interval in the range of 5 to 60 in seconds. If any alarm occurs, the user gets the log message before the specific interval configured by the user. The default value is 5 seconds.
ddm-traps-send	Enables or disables the sending of trap messages. When enabled, the trap message is sent to the Device manager, any time the alarm occurs. The default is enable.

rmon

Configure RMON functions on the switch to set alarms and capture events.

Syntax

rmon

Parameters

Variable	Value
alarm <1-65535> WORD<1-536> <1-3600> {absolute | delta} rising-threshold <-2147483648-2147483647> [<event:1-65535>] falling-threshold <-2147483648-2147483647> [<event:1-65535>] [owner WORD<1-127>] default rmon alarm <1-65535>	Creates an alarm interface. • *<1-65535>* is the interface index number from 1–65535. • **WORD<1-1536>** is the variable name or OID, case sensitive (string length 1–1536). • **{absolute | delta}** is the sample type. • **rising-threshold <-2147483648-2147483647> [<event:1-65535>]** is the rising threshold (–2147483648–2147483647) and the rising event number (1–65535). • **falling-threshold <-2147483648-2147483647> [<event:1-65535>]** is the falling threshold (–2147483648–2147483647) and the falling event number (1–65535). • **owner** <*WORD/2-127*> is the name of the owner (string length 1–48). • *default rmon alarm <65535>* is the default rmon alarm configuration. Use the **no** operator to disable RMON alarms: **no rmon alarm [<1-65535>]**
stats <1-65535> <portList> [owner WORD<1-127>]	Creates an ether-stats control interface. • *<1-65535>* is the index number of the ether stats control interface. • *portList* is the single port interface {slot/port[-slot/port][,...]}. • **owner** *WORD<1-127>* is name of the owner (string length 1–127).

Variable	Value
	Use the **no** operator to delete a stats control interface: **no rmon stats [<1-65535>]**
event <1-65535> [log] [trap] [description <LINE>] [owner <LINE>] [trap_src <A.B.C.D>] [trap_dest <A.B.C.D>] [community WORD<1-127>]	Creates an event. • <*1-65535*> is the event index number. • **[log]** displays information about configured traps. • **[trap]** specifies trap source and destination IP addresses. • **description** <*LINE*> is the event description (string length 0–127). • **owner** <*WORD/1-127*> is the name of the owner (string length 1–127). • **trap_src** <*A.B.C.D*> is the trap source ip address. • **trap_dest** <*A.B.C.D*> is the trap destination ip address. • **community** <*WORD/1-27*> is the event community (string length 1–127). Use the **no** operator to delete a RMON event: **no rmon event [<1-65535>] [log]**
history <1-65535> <portList> [<buckets: 1-65535>][<interval: 1-3600>][owner WORD<1-127>]	Creates a history control interface. • <*1-65535*> is the index number of the history control interface (1–65535). • <*portList*> is the single port interface {slot/port[-slot/port][,...]}. • **[<buckets:1-65535>]** is the number of buckets requested (1–65535). • **[<interval:1-3600>]** is the time interval in seconds over which the data is sampled for each bucket (1–3600). • **[owner <WORD/1-127>]** is the name of the owner (string length 1–48). Use the **no** operator to delete a history control interface: **no rmon history [<1-65535>]**
memsize <250000-4000000>	Configures the amount of RAM in bytes to allocate for RMON. The range is 250000–4000000.

Variable	Value
trap-option <*toOwner*|*toAll*>	Controls whether the RMON traps are sent to the owner or to all trap recipients. **toOwner|toAll** is set to either the owner or to all trap recipients.
util-method <*half*|*full*>	Controls whether port utilization is calculated in half or full duplex.

Default

None

Command mode

Global Configuration mode

show alarm

Displays the contents of the alarm log buffers.

Syntax

show alarm [database|statistics]

Parameters

Variable	Value
database	Displays the alarm database.
statistics	Displays the alarm database statistics.

Default

None

Command mode

Privileged EXEC mode

Related commands

Variable	Value
alarm-id *WORD <0–32>*	Specifies the alarm ID in the range of 0 to 32.
alarm-status *WORD <0–32>*	Sets the alarm status in the range of 0 to 32 characters. Valid options are set or clear.
alarm-type *WORD <0–32>*	Specifies the alarm type as persistent or dynamic. The range is 0 to 32 characters.

Variable	Value
event-code *<0x0–0x0FFFFFF|0x0–0x0>*	Specifies the event code.
module *WORD <0–100>*	Specifies the alarm module. Options available are SNMP|EAP|RADIUS|RMON|WEB|IGMP|HW|MLT|FILTER|QOS|SW|CPU|IP|VLAN|IPMC|IP-RIP|OSPF|PIM|POLICY|RIP.
severity *WORD <0–25>*	Indicates the severity level. Options are INFO|ERROR|WARNING|FATAL.
name-of-file *WORD <1–99>*	Denotes the name of the log file to be displayed in the range of 1 to 99 characters.
save-to-file *WORD <1–99>*	Specifies the filename, /intflash <file>, /extflash <file>, /usbflash <file> in the range of 1 to 99 characters.

show eapol auth-stats interface

Display the Authenticator statistics to manage network performance.

Syntax

show eapol auth-stats interface [gigabitethernet {slot/port [-slot/port][,...]}]

show eapol auth-stats interface vlan <1–4084> [slot/port[-slot/port][,...]

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan *<1–4084>*	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show eapol session interface

View EAPoL session statistics to manage network performance.

Syntax

show eapol session interface [gigabitethernet {slot/port [-slot/port] [,...]}] [vlan <1–4084>]

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan <*1–4084*>	Specifies the VLAN for which to show the statistics.

Default

None

Command mode

Privileged EXEC mode

show eapol session-stats interface

Display the port Extensible Authentication Protocol (EAPOL) authenticator session statistics for the specified interface type.

Syntax

show eapol session-stats interface

show eapol session-stats interface gigabitethernet

show eapol session-stats interface gigabitethernet {slot/port [-slot/port][,...]}

show eapol session-stats interface vlan <1–4084>

show eapol session-stats interface[vlan <1–4084> [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan *<1–4084>*	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show eapol status interface

Display the port Extensible Authentication Protocol (EAPoL) operation statistics for the specified interface type.

Syntax

show eapol status interface

show eapol status interface gigabitEthernet

show eapol status interface gigabitEthernet {slot/port[-slot/port][,...]}

show eapol status interface vlan <1–4084>

show eapol status interface vlan <1–4084> {slot/port[-slot/port][,...]}

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan *<1–4084>*	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1),

Variable	Value
	a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show filter acl statistics

View port statistics to ensure that the ACE operates correctly.

Syntax

show filter acl statistics all

show filter acl statistics default

show filter acl statistics default <1-2048>

show filter acl statistics global

show filter acl statistics global <1-2048>

show filter acl statistics <1-2048> <1–2000>

show filter acl statistics <1-2048> qos

show filter acl statistics <1-2048> security

show filter acl statistics <1-2048>

show filter acl statistics

Parameters

Variable	Value
<1–2048>	Specifies ACL ID.
<1-2048> <1–2000>	Specifies the ACL and the ACE ID.
all	Shows all statistics for all access control entries.
default	Shows traffic statistics for access control entry.
global	Shows global statistics for access control entry.
<1–2048> qos	Shows statistics for QoS access control entries.

Variable	Value
<*1–2048*> security	Shows statistics for Security access control entries.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet

Show configuration information for GigabitEthernet ports.

Syntax

show interfaces gigabitethernet [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet config

Show the configuration for specific ports and VLANs to manage network performance.

Syntax

show interfaces gigabitethernet config [<1–4084>] [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet cp-limit

Show CP-Limit configuration information for the port .

Syntax

show interfaces GigabitEthernet cp-limit [{slot/port [-slot/port] [,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet error

Show general error information for the port.

Syntax

show interfaces GigabitEthernet error [{slot/port [-slot/port] [,...]}]

show interfaces GigabitEthernet error collision [{slot/port [-slot/port][,...]}]

show interfaces GigabitEthernet error ospf [{slot/port [-slot/port] [,...]}]

show interfaces GigabitEthernet error verbose [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Specifies the slot and the port number or a range of ports.
collision	Show port collision error information.
ospf	Show port ospf error information.
verbose	Show port error information. Display priority-based flow control pause transmit and receive counter.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet fdb-entry

Show the forwarding database (FDB) entries for the port.

Syntax

show interfaces gigabitethernet fdb-entry [<1–4084>] [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet high-secure

Show the high-secure configuration for the port.

Syntax

`show interfaces gigabitethernet high-secure [<1–4084>] [{slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet interface

Shows general port information.

Syntax

show interfaces gigabitethernet interface [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet l1–config

Show Layer 1 configuration information for the port.

Syntax

show interfaces gigabitethernet l1–config [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet limit-fdb-learning

Show the configuration for the limit FDB learning feature.

Syntax

show interfaces gigabitEthernet limit-fdb-learning [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet loop-detected

Display loop detection information for the port.

Syntax

show interfaces gigabitEthernet loop-detected [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet mac-security

Show information about the unknown MAC discard feature for the port.

Syntax

show interfaces gigabitEthernet mac-security [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet name

Show port names and general configuration information.

Syntax

show interfaces gigabitEthernet name [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet ospf

Shows OSPF port information.

Syntax

`show interfaces gigabitethernet ospf [<1–4084>] [{slot/port [-slot/port][,...]}]`

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet rate-limit

Show rate-limit configuration information for the port.

Syntax

show interfaces gigabitethernet rate-limit [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet shape

Show the configuration for egress rate-limiting on the port.

Syntax

show interfaces gigabitEthernet shape [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet slpp

Display the SLPP configuration information for the port.

Syntax

show interfaces slpp [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet state

Shows the state of the port.

Syntax

show interfaces gigabitEthernet state [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics

Display individual statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitethernet statistics {slot/port [-slot/port] [,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics bridging

Display individual bridging statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitethernet statistics bridging {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics dhcp-relay

Show DHCP relay information to view DHCP parameter information for one port, for all ports, or for a VLAN.

Syntax

`show interfaces gigabitethernet statistics dhcp-relay {slot/port [-slot/port][,...]} [vrf WORD<0-16>] [vrfids WORD<0-512>]`

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Specifies the slot and the port number.
vrf *WORD<0-16>*	The name of the VRF. The range is 0 to 16.
vrfids *WORD<0–512>*	The ID of the VRF and is an integer. The range is 0–512.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics lacp

Display individual LACP statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitEthernet statistics lacp {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics policer

Display individual policer statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitEthernet statistics policer {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics rmon

Display individual RMON statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitEthernet statistics rmon history {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.
history	Displays RMON history statistics.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet statistics verbose

Display individual verbose statistics for specific ports to manage network performance.

Syntax

show interfaces gigabitEthernet statistics verbose {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by port.

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet vlan

Show VLAN information for the port.

Syntax

show interfaces gigabitEthernet vlan [<1–4084>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces gigabitethernet vrfs

Show VRF-association information for the port..

Syntax

show interfaces gigabitEthernet vrfs [vrf WORD<0–16>] [vrfids WORD<0–512>] [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
vrf *WORD<0–16>*	Specifies a VRF instance by name.
vrfids *WORD<0–512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show interfaces mgmtethernet

Show configuration information for MgmtEthernet ports.

Syntax

`show interfaces mgmtethernet [{slot/port [-slot/port][,...]}]`

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces mgmtethernet config-L1

Show Layer 1 configuration information for the port.

Syntax

`show interfaces mgmtethernet config-l1 [{slot/port [-slot/port] [,...]}]`

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show interfaces mgmtethernet error

Show general error information for the port.

Syntax

show interfaces mgmtethernet error [{slot/port [-slot/port][,...]}]

show interfaces mgmtethernet error collision [{slot/port [-slot/port][,...]}]

show interfaces mgmtethernet error ospf [{slot/port [-slot/port][,...]}]

show interfaces mgmtethernet error verbose [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Specifies the slot and the port number or a range of management ports.
collision	Show management port collision error information.
ospf	Show management port ospf error information.
verbose	Show management port error information. Display priority-based flow control pause transmit and receive counter.

Default

None

Command mode

Privileged EXEC mode

show interfaces mgmtethernet statistics

Display individual statistics for specific management ports to manage network performance.

Syntax

show interfaces mgmtethernet statistics

show interfaces mgmtethernet statistics {slot/port [-slot/port] [,...]}

show interfaces mgmtethernet statistics verbose [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Displays all statistics by management port.
verbose *{slot/port [-slot/port][,...]}*	Displays verbose statistics for specific management ports to manage network performance.

Default

None

Command mode

Privileged EXEC mode

show ip ipfix

View global IPFIX information to see the global administrative state of IPFIX for the chassis.

Syntax

show ip ipfix

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show ip ipfix collector

View collector information to verify the collector configuration.

Syntax

show ip ipfix collector [{slot[-slot][,...]}] [<A.B.C.D>]

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3–12.
{slot[-slot][,...]}<*A.B.C.D*>	Displays the collector info for the IP address and slot.

Default

None

Command mode

Privileged EXEC mode

show ip ipfix export

View the exporter statistics for each slot to see the following information:

- collector IP address
- packets sent since you enabled IPFIX
- bytes sent since you enabled IPFIX
- packets lost within the device
- IPFIX protocol status

If you do not specify a slot, all slots appear in the command output.

Syntax

show ip ipfix export [{slot[-slot][,...]}]

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3–12.

Default

None

Command mode

Privileged EXEC mode

show ip ipfix exporter

View the exporter configuration to show the following information:

- the administrative state of the exporter
- the template refresh rate
- the export interval
- the aging time
- the active timeout value

Syntax

`show ip ipfix exporter [{slot[-slot][,...]}]`

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3-12

Default

None

Command mode

Privileged EXEC mode

show ip ipfix flows

View flow information to see the flow entries. The flow database is large; the functionality is simple in terms of sorting. The response time can be slow for sorted displays.

This command displays records from only one interface module at a time. This command uses the following type of optional fields:

- Fields that specify match fields. These fields can be an exact match or an operator like LE, GE, EQ, NE.

Syntax

show ip ipfix flows {slot[-slot][,...]} [byte-count WORD<1-2> <0-4294967295>] [dest-addr WORD<1-2> {A.B.C.D}] [first-pkt-time WORD<1-2> <MMddyyyyhhmmss>] [last-pkt-time WORD<1-2> <MMddyyyyhhmmss>] [monitor <false|true>] [numflows <0–16000>] [pkt-count WORD<1-2> <0-4294967295>] [port WORD<1-2> {slot/port}] [protocol WORD<1-2> <0–255>] [source-addr WORD<1-2> {A.B.C.D}] [TCP-UDP-dest-port WORD<1-2> <0-65535>] [TCP-UDP-src-port WORD<1-2> <0-65535>] [TOS WORD<1-2> <0–255>] [vlan WORD<1-2> <1–4084>]

Parameters

Variable	Value
byte-count *WORD<1-2> <0-4294967295>*	Shows the flows that match a number of bytes. Use the format oper{=|!=|<=|>=} and byte-count {0-4294967295}; for example, {>=a}.
dest-addr *WORD<1-2> {A.B.C.D}*	Shows the flows for a destination address. Use the format oper{=|!=|<=|>=} and ip address {A.B.C.D}; for example, {<=A.B.C.D}.
first-pkt-time *WORD<1-2> <MMddyyyyhhmmss>*	Shows the flows that match a timestamp for when the flow was first observed. Use the format oper{=|!=|<=|>=} and time {MMddyyyyhhmmss}; for example, {>=a}.
last-pkt-time *WORD<1-2> <MMddyyyyhhmmss>*	Shows the flows that match a timestamp for when the flow was last observed. Use the format oper{=|!=|<=|>=} and time {MMddyyyyhhmmss}; for example, {>=a}.
monitor <false|true>	Monitors the top 10 flows (by byte count) if you configure this variable to true. The maximum number of flows you can monitor is 100.
numflows *<0–16000>*	Shows the number of flows you specify. Specify zero (0) to show a flow summary. If you enter 0, the command output contains two extra lines at the bottom. The first line is all dashes and the second line is the total number of flows based on the slots you specify.

Variable	Value
pkt-count *WORD<1-2> <0-4294967295>*	Shows the flows that match a packet count. Use the format oper{=|!=|<=|>=} and pktcount {0– 4294967295}; for example, {>=a}.
port *WORD<1-2> {slot/port}*	Shows the flows for a particular port. Use the format oper{=|!=|<=|>=} and {slot/port}; for example, {=a/b}.
protocol *WORD<1-2> <0–255>*	Shows the flows for a particular protocol. Use the format oper{=|!=|<=|>=} and protocol {0–255}; for example, {>=a}. The mapping values for some protocol types are: icmp:1, tcp:6, udp:17, ipsecesp:50, ipsecah:51, ospf: 89, vrrp:112, snmp:254, undefined:256.
source-addr *WORD<1-2> {A.B.C.D}*	Shows the flows for a source address. Use the format oper{=|!=|<=|>=} and ip address {A.B.C.D}; for example, {<=A.B.C.D}.
TCP-UDP-dest-port *WORD<1-2> <0-65535>*	Shows the flows for a destination port. Use the format oper{=|!=|<=|>=} and port {0–65535}; for example, {>=a}.
TCP-UDP-src-port *WORD<1-2> <0-65535>*	Shows the flows for a source port. Use the format oper{=|!=|<=|>=} and port {0–65535}; for example, {>=a}.
TOS *WORD<1-2> <0–255>*	Shows the flows that match a type of service. Use the format oper{=|!=|<=|>=} and TOS{0-255}; for example, {>=a}
vlan *WORD<1-2> <1–4084>*	Shows the flows for a particular VLAN. Use the format oper{=|!=|<=|>=} and vlan{1–4084}; for example, {!=10}.

Default

None

Command mode

Privileged EXEC mode

show ip ipfix hash-statistics

View the hashing statistics to view total hash overflows.

If you do not specify a slot, all slots appear in the command output.

Syntax

`show ip ipfix hash-statistics [{slot[-slot][,...]}]`

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6). Valid slots are 3–12.

Default

None

Command mode

Privileged EXEC mode

show ip ipfix interface

View IPFIX information for an interface to see the sampling rate and the IPFIX administrative status for the interface.

Syntax

`show ip ipfix interface [gigabitethernet slot/port[-slot/port] [,...]}]`

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).

Default

None

Command mode

Privileged EXEC mode

show ip mroute stats

View multicast routing process statistics.

Syntax

`show ip mroute stats [WORD<7-160>]`

Parameters

Variable	Value
WORD<7-160>	Specifies the group IP address in the format {A.B.C.D[,E.F.G.H][,...]} . The maximum number of group IP addresses is 10. To view statistics, the group IP address is optional. To monitor statistics, the group IP address is required.

Default

None

Command mode

Privileged EXEC mode

show ip ospf ifstats

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

`show ip ospf ifstats [detail] [mismatch] [vrf WORD<0–16>] [vrfids WORD<0–512>]`

Parameters

Variable	Value
detail	Displays the details of the OSPF.
mismatch	**`mismatch`** is the number of times the area ID is not matched.
vrf *WORD<0–16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0–512>*	Specifies a VRF or range of VRFs by ID.

Default

None

Command mode

Privileged EXEC mode

show ip ospf stats

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

show ip ospf stats [vrf WORD<0–16>] [vrfids WORD<0–512>]

Parameters

Variable	Value
vrf *WORD<0–16>*	Specifies a VRF instance by VRF name.
vrfids*WORD<0–512>*	Specifies a VRF or range of VRFs by ID.

Default

None

Command mode

Privileged EXEC mode

show ip tcp statistics

View TCP statistics to manage network performance.

Syntax

show ip tcp connections

show ip tcp properties

show ip tcp statistics

Parameters

Variable	Value
connections	Displays IP TCP connections information command.

Variable	Value
properties	Displays IP TCP global properties.
statistics	Displays IP TCP global statistics command.

Default

None

Command mode

Privileged EXEC mode

show ip udp statistics

Displays UDP statistics information.

Syntax

show ip udp statistics

show ip udp endpoints

Parameters

Variable	Value
endpoints	Displays IP UDP endpoints information.
statistics	Displays IP UDP statistics information.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp interface gigabitEthernet statistics

Displays statistics for VRRP ports.

Syntax

show ip vrrp interface gigabitEthernet statistics

show ip vrrp interface gigabitEthernet statistics {slot/port[-slot/port][,...]}

Parameters

None.

Default

None

Command mode

Privileged EXEC mode

show ip vrrp statistics

Displays Virtual Router Redundancy Protocol (VRRP) statistics.

Syntax

show ip vrrp statistics [address {A.B.C.D}] [vrf WORD<0–16>] [vrfids WORD<0–512>] [vrid<1–255>]

Parameters

Variable	Value
address *{A.B.C.D}*	Specifies the address of the backup VRRP.
vrf *WORD<0–16>*	Specifies the VRF name.
vrfids *WORD<0–512>*	Specifies the ID of the VRF and is an integer in the range of 0 to 512.
vrid *WORD<1–255>*	Specifies a unique integar value that represents the virtual router ID in the range of 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

Default

None

Command mode

Privileged EXEC mode

show lacp interface

View LACP statistics for each port to monitor LACP performance of the port.

Syntax

show lacp interface <mlt|gigabitethernet> vid <1–4084> {slot/port [-slot/port][,...]}

Parameters

Variable	Value
<mlt|gigabitethernet>	Specifies the interface type for LACP. The ifindex of the MLT ranges from 64 to 6399.
vid *<1–4084>*	Shows only ports attached to a particular VLAN id in the range of 1 to 4084.
{slot/port [-slot/port][,...]}	Specifies the slot and the port number.

Default

None

Command mode

Privileged EXEC mode

show mac-security mac-da-filter

Display the global level MAC addresses to be filtered.

Syntax

show mac-security mac-da-filter

Parameters

Variable	Value
mac-da-filter	Shows the global level MAC addresses to be filtered.

Default

None

Command mode

Privileged EXEC mode

show mlt stats

View MLT statistics to display MultiLinkTrunking statistics for the switch or for the specified MLT ID.

Syntax

`show mlt stats <1–512>`

Parameters

Variable	Value
<1–512>	Specifies the MLT ID. The value ranges from 1–512.

Default

None

Command mode

Privileged EXEC mode

show monitor-statistics

Displays monitor timer configurations, including duration and interval.

Syntax

`show monitor-statistics`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show pcap stats

View PCAP statistics to manage network performance.

Syntax

show pcap stats

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show pluggable-optical-modules

View DDI module information to view SFP and SFP+ manufacturing information and characteristics, temperature and voltage information, and configuration details.

Syntax

show pluggable-optical-modules basic [{slot/port [-slot/port] [,...]}]

show pluggable-optical-modules config

show pluggable-optical-modules detail [{slot/port [-slot/port] [,...]}]

show pluggable-optical-modules temperature [{slot/port [-slot/port] [,...]}]

show pluggable-optical-modules voltage [{slot/port [-slot/port] [,...]}]

Parameters

Variable	Value
basic	Shows basic SFP and SFP+ information.
config	Shows pluggable optical modules configuration information.

Variable	Value
detail	Shows detailed SFP and SFP+ information.
{slot/port [-slot/port][,...]}	Optionally, identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
temperature	Shows SFP and SFP+ temperature information.
voltage	Shows SFP and SFP+ voltage information.

Default

None

Command mode

Privileged EXEC mode

show ports statistics ospf extended

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

`show ports statistics ospf extended {slot/port [-slot/port][,...]}`

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Specifies the slot and the port number or a range of ports.

Default

None

Command mode

Privileged EXEC mode

show ports statistics ospf main

Use statistics to help you monitor Open Shortest Path First (OSPF) performance.

Syntax

show ports statistics ospf main {slot/port [-slot/port][,...]}

Parameters

Variable	Value
{slot/port [-slot/port][,...]}	Specifies the slot and the port number or a range of ports.

Default

None

Command mode

Privileged EXEC mode

show qos statistics policy

Display individual queue statistics with the following procedure.

Syntax

show qos statistics policy <1–16000> slot {slot [-slot][,...]}

Parameters

Variable	Value
<1–16000>	Specifies the policy id in the range of 1 to 16000.
slot *{slot [-slot][,...]}*	Specifies the slot number for statistics collection. The valid slots are between 3 to 12.

Default

None

Command mode

Privileged EXEC mode

show rmon

View RMON settings to see information about alarms, statistics, events, or the status of RMON on the switch.

Syntax

`show rmon [alarm|event|history|log|stats]`

Parameters

Variable	Value
alarm	Displays RMON alarm information on the switch.
event	Displays RMON events information on the switch.
history	Displays RMON history on the switch.
log	Displays RMON log information on the switch.
stats	Displays RMON statistics information on the switch.

Default

None

Command mode

Privileged EXEC mode

show rmon stats

View RMON statistics to manage network performance.

Syntax

`show rmon stats`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show routing statistics

View port routing statistics to manage network performance.

Syntax

show routing statistics interface

show routing statistics interface gigabitethernet [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
gigabitethernet*{slot/port [-slot/port][,...]}*	Indicates the interface type and the slot and the port number.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp port statistics

Displays Multiple Spanning Tree Protocol (MSTP) Multiple Spanning Tree Instance (MSTI) information to ensure the feature is configured correctly for your network.

Syntax

show spanning-tree mstp port statistics [{slot/port [-slot/port] [,...]}]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp statistics

Display MSTP statistics to see MSTP related bridge-level statistics.

Syntax

show spanning-tree mstp statistics

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp port statistics

View the RSTP information for a selected port to display the RSTP related configuration information for the selected port.

Syntax

show spanning-tree rstp port statistics [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Shows RSTP port statistics.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp statistics

View Rapid Spanning Tree Protocol statistics to manage network performance.

Syntax

show spanning-tree rstp statistics

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show sys stats ipmc-threshold-exceeded-cnt

Display IP multicast exceeded threshold counters.

Syntax

show sys stats ipmc-threshold-exceeded-cntshow spf-flags

Parameters

None

Default

None

Command mode

Privileged EXEC mode

Chapter 14: QoS and IP filtering commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to configure Quality of Service (QoS) and filtering operations on the Avaya Virtual Services Platform 9000.

access-diffserv

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted (core) port honors incoming Differentiated Services Code Point (DSCP) markings. An untrusted (access) port overrides DSCP markings.

Syntax

access-diffserv [port {slot/port[-slot/port][,...]}] [enable]

default access-diffserv [port {slot/port[-slot/port][,...]}] [enable]

no access-diffserv [port {slot/port[-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	If enabled, specifies an access port and overrides incoming DSCP bits. If disabled, specifies a core port and honors and handles incoming DSCP bits. The default is disabled.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default configuration is trusted (disabled).

Command mode

GigabitEthernet Interface Configuration mode

enable-diffserv

Enable DiffServ so that the switch provides DiffServ-based QoS on that port.

Syntax

enable-diffserv [port {slot/port [-slot/port][,...]}] [enable]

default enable-diffserv [enable]

no enable-diffserv [enable]

Parameters

Variable	Value
enable	Enables DiffServ for the specified port. The default is disabled.
port *{slot/port [-slot/port][,...]}*	Specifies the slot and port, or slot and port list. To delete the current configuration, use the no option in the command **no enable-diffserv [port <portList>]**

Default

None

Command mode

GigabitEthernet Interface Configuration mode

filter acl

Use an ACL to specify an ordered list of ACEs, or filter rules.

Syntax

filter acl <1-2048> type <inVlan|outVlan|inPort|outPort> [name WORD<0-32>]

Parameters

Variable	Value
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.

Variable	Value
type <inVlan|outVlan|inPort|outPort>	Specifies the ACL type. **inVlan** and **inPort** are ingress ACLs, and **outVlan** and **outPort** are egress ACLs.
<1-2048>	Specifies a unique identifier (1 to 2048) for this ACL.

Default

None

Command mode

Global Configuration mode

filter acl ace

Use an access control entry (ACE) to define a packet pattern and the desired behavior for packets that carry the pattern.

Syntax

filter acl ace <1-2048> <1-2000> [name WORD<1-32]

Parameters

Variable	Value
name *WORD<1-32>*	Specifies an optional descriptive name for the ACE that uses 1–32 characters.
<1-2000>	Specifies an ACE ID from 1 to 2000.
<1-2048>	Specifies an ACL ID from 1 to 2048.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
enable	Enables an ACE within an ACL. After you enable an ACE, to make changes, first disable it.

filter acl ace action

Configure the ACE action mode as deny or permit.

Syntax

filter acl ace action <1-2048> <1-2000> {permit|deny} [copy-to-pcap] [count] [log]

filter acl ace action <1-2048> <1-2000> {permit|deny} [internal-qos <0–7>]

filter acl ace action <1-2048> <1-2000> permit ipfix-enable

filter acl ace action <1-2048> <1-2000> {permit|deny} mlt-index <1-16>

filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ip {A.B.C.D} [dscp <0–63>] [ttl <2–255>]

filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-mlt <1–512>

filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ports {slot/port[-slot/port][,...]}]

filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-vlan <1-4084>

filter acl ace action <1-2048> <1-2000> {permit|deny} [police <1-16000>]

filter acl ace action <1-2048> <1-2000> {permit|deny} [redirect-next-hop WORD<1-15>]

filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dot1p <0–7>]

filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dscp {0..63}]

filter acl ace action <1-2048> <1-2000> {permit|deny} [unreachable <deny|permit>]

default filter acl ace action <1-2048> <1-2000> {permit|deny}

default filter acl ace action <1-2048> <1-2000> {permit|deny} [copy-to-pcap] [count] [log]

default filter acl ace action <1-2048> <1-2000> {permit|deny} [internal-qos]

default filter acl ace action <1-2048> <1-2000> permit ipfix-enable

default filter acl ace action <1-2048> <1-2000> {permit|deny} mlt-index

default filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ip [dscp] [ttl]

default filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-mlt

default filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ports

default filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-vlan

default filter acl ace action <1-2048> <1-2000> {permit|deny} [police]

default filter acl ace action <1-2048> <1-2000> {permit|deny} [redirect-next-hop]

default filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dot1p]

default filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dscp]

default filter acl ace action <1-2048> <1-2000> {permit|deny} [unreachable]

no filter acl ace action <1-2048> <1-2000> {permit|deny}

no filter acl ace action <1-2048> <1-2000> {permit|deny} [copy-to-pcap] [count] [log]

no filter acl ace action <1-2048> <1-2000> {permit|deny} [internal-qos]

no filter acl ace action <1-2048> <1-2000> permit ipfix-enable

no filter acl ace action <1-2048> <1-2000> {permit|deny} mlt-index

no filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ip [dscp] [ttl]

no filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-mlt

no filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-ports

no filter acl ace action <1-2048> <1-2000> {permit|deny} monitor-dst-vlan

no filter acl ace action <1-2048> <1-2000> {permit|deny} [police]

no filter acl ace action <1-2048> <1-2000> {permit|deny} [redirect-next-hop]

no filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dot1p]

no filter acl ace action <1-2048> <1-2000> {permit|deny} [remark-dscp]

Parameters

Variable	Value
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
<1-2048>	Specifies an ACL ID from 1 to 2048.
copy-to-pcap	This variable is a security action that sends a copy of the packet to the secondary CP module. The ACE ID must be in the range of 1–1000. The default is disabled.
count	Enables the ability to count matching packets. Use this parameter with either a security or QoS ACE. The default is disabled.
<permit|deny>	Configures the action mode for security ACEs. Each ACE has a mode of permit or deny the matched traffic. You can use filters to configure metering of permitted traffic. If you need to enable IPFIX on denied traffic, you must enable it on an individual port basis, which enables IPFIX monitoring on all traffic that enters a port. **Note:** For each Security ACE (1-1000), you must define one or more actions as well as the associated action mode (permit or deny). Otherwise, the security ACE cannot be enabled. There is no default configuration for Security ACEs. With QoS ACEs (1001-2000), the action mode is not configurable. QoS ACEs are always set to action mode permit.
internal-qos	This variable is a QoS action. The ACE ID must be in the range of 1001–2000. The default value is 1.
ipfix-enable	Enables IPFIX metering. The default is disabled.
log	This action logs to the master CP module. Use this parameter with either a security or QoS ACE. The default is disabled.

Variable	Value
mlt-index *<1-16>*	If you use this action, the ACE overrides the mlt-index chosen by the MLT algorithm for packets sent on MLT ports. The MLT index ranges from 1–16. If three ports exist in an MLT (for example, A, B, and C) and you specify an index of 6, the Virtual Services Platform 9000 applies the MOD function and chooses port C. If port C becomes nonoperational, the filtered packets exit the platform from port B. Multicast traffic does not support the MLT index. This variable is a security action. The ACE ID must be in the range of 1–1000.
monitor-dst-ip {A.B.C.D} [dscp<0–63>] [ttl <2–255>]	Configures Layer 3 mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 256 (disabled) and the default TTL is 64. For Layer 3 mirroring, every hop in the path from the mirrored port to the remote-mirroring port must be routed. Avaya recommends that you configure the remote-mirrored port in its own VLAN at the last hop to prevent flooding.
monitor-dst-mlt *<1–512>*	Configures mirroring to a destination MLT group. This action is a security action. The ACE ID must be in the range of 1– 1000.
monitor-dst-ports {slot/port[- slot/port][,...]}	Configures mirroring to a destination port or ports. This action is a security action. The ACE ID must be in the range of 1–1000. {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2)
monitor-dst-vlan *<1–4084>*	Configures mirroring to a destination VLAN. This action is a security action. The ACE ID must be in the range of 1– 1000.
police *<1-16000>*	Polices the packet according to the specified policy ID (1– 16000). A policy must exist. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
redirect-next-hop *WORD<1-15>*	Specifies the next-hop IP address for redirect mode (a.b.c.d). This action is a security action. The ACE ID must be in the range of 1–1000.

Variable	Value
remark-dot1p <*0–7*>	Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
remark-dscp <*0–63*>	Specifies the new Per-Hop Behavior (PHB) for matching packets: phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41, phbaf42, phbaf43, phbcs5, phbef, phbcs6, phbcs7. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
unreachable <deny|permit>	Denies or permits packet dropping when the next-hop for the packet is unreachable. The default value is deny. This action is a security action. The ACE ID must be in the range of 1–1000.

Default

The default to configure ACE actions to meter flows after a packet matches an ACE is disabled.

There is no default configuration for Security ACEs (1–1000). With QoS ACEs (1001-2000), the action mode is not configurable. QoS ACEs are always set to action mode permit.

Command mode

Global Configuration mode

filter acl ace arp

Use ACE ARP entries so that the filter looks for ARP requests or responses.

Syntax

filter acl ace arp <1-2048> <1-2000> operation eq <arprequest|arpresponse>

default filter acl ace arp <1-2048> <1-2000> operation eq <arprequest|arpresponse>

no filter acl ace arp <1-2048> <1-2000> operation eq <arprequest|arpresponse>

Parameters

Variable	Value
operation eq <arprequest| arpresponse>	Specifies an ARP operation type of arpRequest or arpResponse. For ARP, only one operator and attribute exist (eq and operation).

Default

None

Command mode

Global Configuration mode

filter acl ace ethernet

Use Ethernet ACEs to filter on Ethernet parameters.

Syntax

`filter acl ace ethernet <1-2048> <1-2000>`

Parameters

Variable	Value
dst-mac <eq|mask> *WORD<1-1024>*	The **<eq|mask>** parameter specifies an operator for a field match condition. The **WORD<1-1024>** parameter specifies a list of destination MAC addresses separated by a comma, or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].
ether-type <eq> *WORD<1-200>*	The **<eq>** parameter specifies an operator for a field match condition: equal to. The **WORD<1-200>** parameter specifies an ether-type name: • ip, arp, ipx802dot3, ipx802dot2, ipxSnap, ipxEthernet2, appleTalk, AppleTalk-Arp, sna802dot2, snaEthernet2, netBios, xns, vines, ipV6, rarp, PPPoE-discovery, or PPPoE-session.
port eq <*slot/port*>	Specifies ports to which to match, where **<slot/port>** specifies the ports.
src-mac <eq|mask> *WORD<1-1024>*	The **<eq|mask>** parameter specifies an operator for a field match condition: equal to.

Variable	Value
	The **WORD<1-1024>** parameter specifies a list of source MAC addresses separated by separated by a comma, or a range of MAC addresses specified from low to high; for example, [AA:BB:CC:DD:EE:FF].
vlan-id <eq|mask> *<1-4084>*	Specifies VLANs to match, where **<1-4084>** specifies the VLAN IDs.
vlan-tag-prio <eq|mask> *<0-7>*	The **<eq|mask>** parameter specifies an operator for a field match condition. The **<0-7>** parameter specifies a VLAN tag priority from 0–7 or undefined.

Default

None

Command mode

Global Configuration mode

filter acl ace ip

Use IP ACEs to filter on the source IP address, destination IP address, DiffServ Code Point (DSCP), protocol, IP options, and IP fragmentation parameters.

Syntax

filter acl ace ip <1-4096> <1-1000> dst-ip eq WORD <1-1024>

Parameters

Variable	Value
dst-ip <eq|mask> *WORD <1-1024>*	The **<eq|mask>** parameter specifies an operator for a field match condition. The **WORD<1-1024>** parameter specifies the destination IP address list in one of the following formats: a.b.c.d, [w.x.y.z-p.q.r.s], [l.m.n.o/mask], [a.b.c.d/len].
dscp <eq|mask> *WORD <0-256>*	The **<eq|mask>** parameter specifies an operator for a field match condition. The equals to parameter specifies the PHB name or DSCP value {0 to 256, where 256 => disable}, or phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41, phbaf42, phbaf43, phbcs5, phbcs6, phbef, or phbcs7.

Variable	Value
ip-frag-flag eq <noFragment| anyFragment>	The **eq** parameter specifies an operator for a field match condition: equal to. The **ip-frag-flag** parameter specifies a match option for IP fragments: noFragment or anyFragment.
ip-options any	Matches to an IP option. Any is the only option.
ip-protocol-type <eq> *WORD <1-256>*	The **<eq>** parameter specifies an operator for a field match condition: equal to. The **WORD<1-256>** parameter specifies one or more IP protocol types: (1–256), or icmp, tcp, udp, ipsecesp, ipsecah, ospf, vrrp, undefined.
src-ip <eq|mask> *WORD <1-1024>*	The **<eq|mask>** parameter specifies an operator for a field match condition: equal to, not equal to, less than or equal to, greater than or equal to. The **WORD<1-1024>** parameter specifies a source IP address list in one of the following formats: a.b.c.d, [w.x.y.z-p.q.r.s], [l.m.n.o/mask], [a.b.c.d/len].

Default

None

Command mode

Global Configuration mode

filter acl ace protocol

Use protocol ACEs to filter on the TCP source port, UDP source port, TCP destination port, UDP destination port, ICMP message type, and TCP flags.

Syntax

filter acl ace protocol <1-2048> <1-2000> icmp-msg-type eq WORD <1-200>

Parameters

Variable	Value
icmp-msg-type <eq> *WORD <1-200>*	Specifies the icmp message type attribute of the protocol. The **<eq>** parameter specifies an operator for a field match condition: equal to. The **WORD<1-200>** parameter specifies one or more IP protocol types (0–255), or {echoreply| destunreach| sourcequench| redirect| echo-request| routeradv|

Variable	Value
	routerselect| time-exceeded| param-problem| timestamp-request| timestamp-reply| addressmask-request| addressmask-reply| traceroute}.
dst-port <eq|mask> *WORD<1-60>*	The **<eq|mask>** parameter specifies an operator for a field match condition: equal to. The **WORD<1-60>** parameter specifies the destination port for the TCP protocol: (0–65535), or {echo| ftpdata| ftpcontrol| ssh| telnet| dns| http| bgp| hdot323| bootpServer| boorpClient| tftp| rip| rtp| rctp| undefined}.
tcp-flags <eq|mask> *WORD<1–50>*	Specifies tcp—flags attribute of [protocol. The **<eq|mask>** parameter specifies an operator for a field match condition. The **WORD <1–50>** parameter specifies one or more TCP flags: {none| fin| syn| rst| push| ack| urg| undefined}. The tcp-flags and icmp-msg-type command options support lists.
src-port <eq|mask> *WORD<1-65535>*	The **<eq|mask>** parameter specifies an operator for a field match condition. The **WORD <1-65535>** parameter specifies the destination port for the TCP protocol {0–65535}.

Default

None

Command mode

Global Configuration mode

filter acl enable

Enable the ACL on the filter.

Syntax

filter acl <1-2048> enable

Parameters

Variable	Value
<1-2048>	Specifies the ACL ID int he range of 1 to 2048.
enable	Enables the ACL state, and all associated ACEs.

Default

The default state is enable.

Command mode

Global Configuration mode

filter acl log buffer-wrap

Enable buffer wrap on filter log.

Syntax

filter acl log buffer-wrap

Parameters

None

Default

None

Command mode

Global Configuration mode

filter acl port

Associate ports with, or remove ports from, an ACL so that filters do or do not apply to port traffic, respectively.

Syntax

filter acl port <1-2048> {slot/port [-slot/port][,...]}

Parameters

Variable	Value
<1–2048>	Specifies an ACL ID from 1–2048.
{slot/port [-slot/port][,...]}	Associates a port or a port list to a particular ACL.

Default

None

Command mode

Global Configuration mode

filter acl set

Configure an Access Control List (ACL) filter.

Syntax

filter acl set <1-2048> default-action [permit|deny] global-action [monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port [-slot/port] [,...]}|monitor-dst-vlan <1-4084>]

filter acl set <1–2048> global-action {ipfix-enable|monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port [-slot/port][,...]}|monitor-dst-vlan <1-4084>}

default filter acl set <1–2048> global-action [ipfix-enable|monitor-dst-mlt |monitor-dst-ports|monitor-dst-vlan]

no filter acl set <1–2048> global-action {ipfix-enable|monitor-dst-mlt |monitor-dst-ports|monitor-dst-vlan}

Parameters

Variable	Value
default-action <permit|deny>	Specifies the action to be taken when none of the ACEs match. The options are deny or permit.
<1–2048>	This is the ACL ID. The range is from 1–2048.
global-action{ipfix-enable| monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port [-slot/port] [,...]}|monitor-dst-vlan <1-4084>}	Specifies the action to be taken for all ACE matches. The options are: ipfix-enable|monitor-dst-mlt <1-512>| monitor-dst-ports {slot/port [-slot/port][,...]}|monitor-dst-vlan <1-4084> *<1–512>* specifies the MLT ID. {slot/port [-slot/port][,...]} specifies the slot and the port number. *<1–4084>* specifies the VLAN ID.

Default

The default action is deny. IPFIX is disabled by default.

Command mode

Global Configuration mode

filter acl vlan

Associate VLANs with, or remove VLANs from, an ACL so that filters do or do not apply to VLAN traffic, respectively.

Syntax

`filter acl vlan <1-2048> <1-4084>`

Parameters

Variable	Value
<1–2048>	Specifies an ACL ID from 1–2048.
<1-4084>	Specifies the VLAN IDs from 1–4084.

Default

None

Command mode

Global Configuration mode

qos 802.1p-override

Configure a port as untrusted to determine the Layer 2 QoS actions the switch performs. An untrusted port (override enabled) overrides 802.1p bit markings.

Syntax

`qos 802.1p-override [enable]`

`default qos 802.1p-override [enable]`

`no qos 802.1p-override [enable]`

Parameters

Variable	Value
enable	If you configure this variable, it overrides incoming 802.1p bits; if you do not configure this variable, it honors and handles incoming 802.1p bits. The default is disable (Layer 2 trusted).

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration mode

qos egressmap

Modify the egress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Syntax

qos egressmap 1p <0-7> <0-7> ds <0–7> WORD <1–6>

default qos egressmap 1p

Parameters

Variable	Value
1p *<0–7>*	Maps the QoS level to IEEE 802.1p priority. Each QoS level has a default IEEE 1P value: • level 0—1 • level 1—0 • level 2—2 • level 3—3 • level 4—4 • level 5—5 • level 6—6 • level 7—7
<0–7>	Specifies the QoS level in the range of 0 to 7.
ds *<0–7>*	Maps QoS level to DS byte.
WORD<1–6>	Specifies the DiffServ code point in hexadecimal, binary, or decimal.

Default

None

Command mode

Global Configuration mode

qos if-policer

Configure a port policer to limit incoming traffic. The switch drops or remarks violating traffic.

Syntax

qos if-policer [port {slot/port [-slot/port][,...]}] peak-rate <64–10000000> svc-rate <64–10000000>

no if-policer port {slot/port [-slot/port][,...]}

default if-policer port {slot/port [-slot/port][,...]}

Parameters

Variable	Value
peak-rate <*64–10000000*>	Specifies the peak rate limit in Kbps. The range is 64–10000000.
port *{slot/port [-slot/port][,...]}*	Specifies the slot and port or slot and portlist.
svc-rate<*64–10000000*>	Specifies the service rate limit in Kbps. The range is 64–10000000.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

qos if-shaper

Configure port-based shaping to rate-limit all outgoing traffic to a specific rate.

Syntax

qos if-shaper [port {slot/port [-slot/port][,...]}] shape-rate <10000–10000000>

no if-shaper port {slot/port}

default if-shaper port {slot/port}

Parameters

Variable	Value
port *{slot/port}*	Specifies the slot and port, or slot and portlist.
shape-rate *<10000-10000000>*	Configures the shaping rate from 10000–10000000 Kb/s.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

qos ingressmap

Modify the ingress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Syntax

`qos ingressmap1p <0-7> <0-7> ds <0–63> <0–7>`

`default qos ingressmap 1p`

Parameters

Variable	Value
`1p <0-7> <0-7>`	Maps the IEEE 802.1p bit to QoS level. Each QoS level has a default IEEE 1P value: • level 0—1 • level 1—0 • level 2—2 • level 3—3 • level 4—4 • level 5—5 • level 6—6 • level 7—7
`ds <0-63> <0-7>`	Maps the DS byte to QoS level.

Default

None

Command mode

Global Configuration mode

qos level port

Configure the default port QoS level to assign a default QoS level for all traffic (providing the packet does not match an ACL that remarks the packet).

Syntax

qos level [port <slot/port>] <0-6>

default qos level

Parameters

Variable	Value
<0-6>	Specifies the default QoS level for the port traffic. QoS level 7 is reserved for network control traffic.
port <*slot/port*>	Specifies the slot and port, or slot and port list.

Default

The default value is 1.

Command mode

Global Configuration mode

qos policy

Configure a QoS policy to configure peak and service policing rates for specific lane members.

Syntax

qos policy <1-16000> peak-rate <64-5000000> svc-rate <64-5000000> [name WORD<1-32>]

Parameters

Variable	Value
<1–16000>	Specifies the policer ID number.
peak-rate *<64-5000000>*	Configures the policer peak rate in Kbps.
svc-rate *<64-5000000>*	Configures the policer service rate in Kbps.
name *WORD<1–32>*	Names the policer template.

Default

None

Command mode

Global Configuration mode

rate-limit

Configure broadcast and multicast bandwidth limiting to limit the amount of ingress broadcast and multicast traffic on a port. The switch drops traffic that violates the bandwidth limit.

Syntax

rate-limit [port {slot/port[-slot/port][,...]}] broadcast <1-65535>

rate-limit [port {slot/port[-slot/port][,...]}] multicast <1-65535>

default rate-limit [port {slot/port[-slot/port][,...]}] broadcast

default rate-limit [port {slot/port[-slot/port][,...]}] multicast

no rate-limit [port {slot/port[-slot/port][,...]}] broadcast

no rate-limit [port {slot/port[-slot/port][,...]}] multicast

Parameters

Variable	Value
<1-65535>	Specifies the bandwidth limit for broadcast and multicast traffic from 1–65535 packets per second
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is disabled (no rate limit).

Command mode

GigabitEthernet Interface Configuration mode

show filter acl

Display filter ACL configuration information.

Syntax

show filter acl <1-2048>

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl ace

Display the filter ACL ACE configuration information.

Syntax

show filter acl ace [<1-2048>] [<1-2000>]

Parameters

Variable	Value
<1-2000>	Specifies an ACE ID from 1 to 2000.
<1-2048>	Specifies an ACL ID from 1 to 2048.

Default

None

Command mode

Privileged EXEC mode

show filter acl action

Display the filter ACL advanced information.

Syntax

show filter acl action [<1-2048>] [<1-2000>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl arp

Display the filter ACL ARP operation configuration information.

Syntax

show filter acl arp [<1-2048>] [<1-2000>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl config

Review your configuration to ensure that it is correct.

Syntax

show filter acl config [<1-2048>] [<1-2000>]

Parameters

Variable	Value
<1–2000>	Specifies an ACE ID from 1–2000.
<1-2048>	Specifies an ACL ID from 1–2048.

Default

None

Command mode

Privileged EXEC mode

show filter acl ethernet

Display the filter ACL Ethernet configuration information.

Syntax

`show filter acl ethernet [<1-2048>] [<1-2000>]`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl ip

Display the filter ACL IP configuration information.

Syntax

`show filter acl ip [<1-2048>] [<1-2000>]`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl log

Display the filter ACL debug configuration information.

Syntax

show filter acl log {slot/port [slot/port][,...]} [<1-2048>] [<1-2000>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show filter acl protocol

Display the filter ACL protocol configuration information.

Syntax

show filter acl protocol [<1-2048>] [<1-2000>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show qos 802.1p-override

Displays the 802.1p override status for a port or VLAN.

Syntax

show qos 802.1p-override gigabitethernet {slot/port[-slot/port][,...]}

show qos 802.1p-override vlan <1–4084>

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show qos egressmap

Display the Quality of Service (QoS) egress mappings.

Syntax

show qos egressmap

show qos egressmap 1p [<0–7>]

show qos egressmap ds [<0–7]

Parameters

Variable	Value
1p	Displays the QoS level to IEEE 802.1p priority mapping.
ds	Displays the QoS level to DS byte mapping.
1p*<0–7>*	Displays the QoS level to IEEE 802.1p priority mapping. Specifies the QoS level. Each QoS level has a default IEEE 1P value: • level 0 – 1 • level 1 — 0

Variable	Value
	• level 2 — 2 • level 3 — 3 • level 4 — 4 • level 5 — 5 • level 6 — 6 • level 7 — 7 The system reserves level 7 for Network Control.
ds<*0–7*>	Displays the QoS level to DS byte mapping. Each QoS level has a default DSCP mapping: • level 0 – 0 • level 1 — 0 • level 2 — 10 • level 3 — 18 • level 4 — 26 • level 5 — 34 • level 6 — 46 • level 7 — 46

Default

None

Command mode

Privileged EXEC mode

show qos ingressmap

Ensure the accuracy of the ingress configuration.

Syntax

show qos ingressmap

show qos ingressmap 1p [<0–7>]

show qos ingressmap ds [<0–63]

Parameters

Variable	Value
1p	Displays the IEEE 802.1p to QoS level mapping.
ds	Displays the DS byte to QoS level mapping.
1p <*0–7*>	Specifies the ingress 802.1p level. Each 802.1p level has a default QoS value: • level 0 – 1 • level 1 — 0 • level 2 — 2 • level 3 — 3 • level 4 — 4 • level 5 — 5 • level 6 — 6 • level 7 — 7
ds<*0–63*>	Displays the DS byte to QoS level mapping. <*0–63*> specifies the Diff-Serv code point (DSCP). To view an extended list of default ingress DSCP to QoS mapping values, see *Avaya Virtual Services Platform 9000 Configuration — QoS and ACL-Based Traffic Filtering*, NN46250–502.

Default

None

Command mode

Privileged EXEC mode

show qos policer

Displays ingress rate-limiting information for an interface.

Syntax

show qos policer interface gigabitethernet [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show qos policy-config

Ensure the accuracy of the QoS policy configuration.

Syntax

show qos policy-config [<1–16000>]

Parameters

Variable	Value
<1-16000>	Specifies the policer ID number.

Default

None

Command mode

Privileged EXEC mode

show qos shaper

Displays egress rate-limiting information for an interface.

Syntax

show qos shaper interface gigabitethernet [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

Chapter 15: Security commands

This chapter describes Avaya Command Line Interface (ACLI) commands to configure security services for the Avaya Virtual Services Platform 9000.

eapol

Configures EAPoL on a specific port when you do not want EAPol applied globally.

Syntax

eapol max-request <1-10>

eapol quiet-interval <1-65535>

eapol re-authentication [enable]

eapol re-authentication-period <1-2147483647>

eapol server-timeout <1-65535>

eapol status authorized

eapol status auto

eapol status unauthorized

eapol supplicant-timeout <1-65535>

eapol traffic-control in

eapol traffic-control in-out

eapol transmit-interval <1-65535>

Parameters

Variable	Value
port *{slot/port [-slot/port][,...]}*	Specifies the port or list of ports used by EAPol. Specify the port list using the following format: {slot/port[-slot/port][, ...]}.
max-request *<1-10>*	Maximum EAP requests sent to supplicant before timing out the session.

Variable	Value
quiet-interval <*1-65535*>	Time interval in seconds between authentication failure and start of a new authentication.
re-authentication enable	Enables reauthenticating an existing supplicant at a specified time interval.
re-authentication-period <*1-2147483647*>	Time interval in seconds between successive reauthentications.
server-timeout <*1-65535*>	Time in seconds to wait for a response from RADIUS server.
sess-manage-mode enable	Enables the port session to be managed by an external device.
sess-manage-open-immediate enable	Sets the port to be opened immediately after 8021x authentication.
status {authorized|auto|unauthorized}	Set the desired EAP authentication status for this port.
supplicant-timeout <*1-65535*>	Time in seconds to wait for response from supplicant for all EAP packets except EAP Request/Identity.
traffic-control {in|in-out}	Desired level of traffic control of port.
transmit-interval <*1-65535*>	Time in seconds to wait for response from supplicant for EAP Request/Identity packets.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

eapol enable

Configure EAPoL on the Virtual Services Platform 9000.

Syntax

`eapol enable`

Parameters

None

Default

None

Command mode

Global Configuration mode

eapol init

Initializes Extensible Authentication Protocol (EAP) administration traffic control direction.

Syntax

`eapol init`

`eapol re-authenticate`

Parameters

Variable	Value
init *{slot/port [-slot/port] [,...]}*	Initializes Extensible Authentication Protocol (EAP) administration traffic control direction.
re-authenticate *{slot/port [-slot/port] [,...]}*	Starts re-authentication immediately.

Default

None

Command mode

Privileged EXEC mode

eapol sess-manage enable

Enable the device to communicate through EAPoL and globally enable the session management.

Syntax

`eapol sess-manage enable`

Parameters

Variable	Value
sess-manage enable	Enables the session management on EAPoL.

Default

None

Command mode

Global Configuration mode

eapol status

Enable EAPoL on an interface.

Syntax

`eapol status {authorized|auto|unauthorized}`

Parameters

Variable	Value
authorized	Specifies the port is always authorized.
auto	Specifies that port authorization depends on the results of the EAPoL authentication by the RADIUS server.
unauthorized	Specifies the port is always unauthorized.

Default

None

Command mode

Global Configuration mode

high-secure enable

Protect the Virtual Services Platform 9000 against IP packets with illegal IP addresses such as loopback addresses or a source IP address of ones, or Class D or Class E addresses from being routed.

Syntax

`high-secure enable`

`default high-secure enable`

`no high-secure enable`

Parameters

Variable	Value
enable	Enables the high secure feature that blocks packets with illegal IP addresses. This flag is disabled by default. Use the **no** operator to remove this configuration.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
port*{slot/port [-slot/port][,...]}*	Specifies ports that must be changed.

ip directed-broadcast

Configure the device to forward directed broadcasts for a VLAN.

Syntax

`ip directed-broadcast [enable]`

`default ip directed-broadcast [enable]`

`no ip directed-broadcast [enable]`

Parameters

Variable	Value
enable	Allows the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

Default

The default is enabled.

Command mode

Interface Configuration mode

ip rvs-path-chk

You can enable, disable or reset the unicast reverse path checking feature to its default setting.

The unicast reverse path checking feature can reduce problems associated with malformed or spoofed IP source addresses in a network.

Syntax

```
[default] [no] ip rvs-path-chk
```

Parameters

Variable	Value
default	Sets the reverse path checking feature to the default setting.
no	Disables the reverse path checking feature.

Default

The ip rvs-path-chk default status is disabled.

Command mode

VLAN and GigabitEthernet Interface Configuration modes

ip rvs-path-chk mode port

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network.

Syntax

`ip rvs-path-chk mode <exist-only|strict>`

Parameters

Variable	Value
`mode` *<exist-only|strict>*	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path

Variable	Value
	checking checks whether the source IP address of the incoming packet exists in the routing table. To set this option to the default value, use the **default** operator with the command.

Default

The ip rvs-path-chk mode port default is exist-only.

Command mode

VLAN and GigabitEthernet Interface Configuration mode

ip rvs-path-chk mode vlan

Use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network.

Syntax

ip rvs-path-chk mode <exist-only|strict>

Parameters

Variable	Value
mode *<exist-only|strict>*	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. To set this option to the default value, use the **default** operator with the command.

Default

The ip rvs-path-chk mode vlan default is exist-only.

Command mode

VLAN Interface Configuration mode

load-encryption-module

Load the appropriate SNMPv3 encryption module before you can use SNMPv3 with Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to access the device.

Syntax

load-encryption-module <3DES|DES|AES>

Parameters

Variable	Value
3DES|DES|AES	Specify the SNMPv3 encryption module to load: 3DES| AES| DES.

Default

None

Command mode

Global Configuration mode

lock port

Lock a port to prevent other users from changing port parameters or modifying port action.

Syntax

lock port {slot/port[-slot/port][,...]} enable

no lock port {slot/port[-slot/port][,...]} enable

Parameters

Variable	Value
port*{slot/port [-slot/port][,...]}*	Specifies the slot and the port number to be locked.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

password aging-time

Configure the duration of your password for when it expires.

Syntax

password aging-time day <1–365>

Parameters

Variable	Value
access level *WORD<2-8>*	Allows or blocks this access level. • no password access-level <WORD 2-8>
aging-time *day <1-365>*	Specifies the number of days that the password is enabled. • *day* has a configurable range of 1–365.
default-lockout-time *<60-65000>*	Changes the default lockout time after three invalid attempts. • *secs* is the lockout time in seconds and is in the range of 60 to 6500. The default is 60 seconds.
lockout *{A.B.C.D| ipv6addr} [time <60-65000>]*	Sets the host lockout time. • *A.B.C.D* is the host IP address. • *ipv6addr* is the IP address for ipv6 address. • *time* is the lockout-out time in seconds for passwords lockout in the range of 60 to 65000. The default is 60 seconds.
min-passwd-len *<10-20>*	Sets the minimum length for passwords in high-secure mode. The range is from a minimum of 10 to 20.
password-history *<3-32>*	Specifies the number of previous passwords to remember. • Password-history has a configurable range of 3 to 32. The default is 3.

Default

None

Command mode

Global Configuration mode

portlock enable

Enable port locking for the security of the ports from any modifications.

Syntax

`portlock enable`

Parameters

Variable	Value
enable	Enables the port locking globally.

Default

None

Command mode

Global Configuration mode

radius

Configure RADIUS to authenticate users identity through a central database.

Syntax

`radius`

Parameters

Variable	Value
accounting {attribute-value <192–240>|enable|include-cli-commands}	Enables RADIUS accounting. The default is false.
access-priority-attribute <*192-240*>	Specifies the value of the Access Priority attribute.in the range of 192 to 240 and the default is 192.
auth-info-attr-value <*0-255*>	Specifies the value of the authentication-information attribute in the range of 0 to 255.The default is 91.
clear-stat	Clears the RADIUS statistics.

Variable	Value
command-access-attribute *<192-240>*	Specifies the value of the command access attribute in the range of 192 to 240 and the default is 194.
cli-commands-attribute *<192-240>*	Specifies the value of the ACLI commands attribute in the range of 192 to 240 and the default is 195.
maxserver*<1–10>*	Specific to RADIUS authentication. Sets the maximum number of servers allowed for the device. The range is between 1 and 10. The default is 10.
mcast-addr-attr-value *<0-255>*	Specifies the value of the multicast address attribute in the range of 0 to 255. The default is 90.

Default

None

Command mode

Global Configuration mode

radius cli-cmd-count

Configure a RADIUS accounting interim request to create a log whenever more than forty CLI commands are executed.

Syntax

`radius cli-cmd-count <1-40>`

Parameters

Variable	Value
<1-40>	Specifies a value of the ACLI command count in the range of 1 to 40.

Default

The default value is 40.

Command mode

Global Configuration mode

radius cli-profile

Use RADIUS ACLI profiling to grant or deny ACLI command access to users being authenticated by way of the RADIUS server.

Syntax

`radius cli-profile`

Parameters

None

Default

The default is disabled/false.

Command mode

Global Configuration mode

radius command-access-attribute

Configure RADIUS authentication and RADIUS accounting attributes to determine the size of the packets received.

Syntax

`radius command-access-attribute <192-240>`

Parameters

Variable	Value
command-access-attribute *<192-240>*	Specifies the RADIUS authentication attribute value is an integer value of the ACLI command count in the range of 192 to 240.

Default

The default value is 192.

Command mode

Global Configuration mode

radius enable

Enable or disable RADIUS authentication globally on the device to allow further configuration to take place.

Syntax

radius enable

Parameters

None.

Default

None

Command mode

Global Configuration mode

radius server host

Add a RADIUS server to allow RADIUS service on the Virtual Services Platform 9000.

Syntax

radius server host WORD<0-46> key WORD<0-32>

radius server host WORD<0-46> key WORD<0-32> [acct-enable|acct-port<1–65536>|enable|port <1–65536>|priority <1–10>|retry <0–6>|source-ip WORD<0–46>|timeout <1–20>]

radius server host WORD<0-46> key WORD<0-32> [used-by cli|used-by eapol|used-by snmp|used-by web]

radius server host WORD<0-46> used-by cli

radius server host WORD<0-46> used-by cli [acct-enable|acct-port <1–65536>|enable|key WORD<0–20>|port <1–65536>|priority <1–10>|retry <0–6>|source-ip WORD<0–46>|timeout <1–20>

radius server host WORD<0-46> used-by eapol

radius server host WORD<0-46> used-by snmp

radius server host WORD<0-46> used-by web

default radius server host WORD<0-46> used-by cli

default radius server host WORD<0-46> used-by cli [acct-enable|acct-port|enable|key|port |priority |retry |source-ip |timeout]

default radius server host WORD<0-46> used-by eapol

default radius server host WORD<0-46> used-by snmp

default radius server host WORD<0-46> used-by web

no radius server host WORD<0-46> used-by cli

no radius server host WORD<0-46> used-by cli [acct-enable|acct-port|enable]

no radius server host WORD<0-46> used-by eapol

no radius server host WORD<0-46> used-by snmp

no radius server host WORD<0-46> used-by web

Parameters

Variable	Value
host *WORD <0–46>*	Create a host server. RADIUS supports IPv4 and IPv6 addresses. WORD <0–46> specifies an address in A.B.C.D or x:x:x:x:x:x:x:x format.
key *WORD<–32>*	Specify a secret key in the range of 0-20 characters.
used-by {cli|snmp|eapol|web}	Specify how the server functions: • cli—configure the server for CLI authentication. • snmp—configure the server for SNMP authentication. • eapol—configure the server for EAPol authentication. • web—configure the server for web authentication.
acct-enable	Enables RADIUS accounting on this server.
acct-port *<1-65536>*	Specify a UDP port of the RADIUS accounting server.
enable	Enables this server.
port *<1-65536>*	Specify a UDP port of the RADIUS server.
priority *<1-10>*	Specify the priority value for this server.
retry *<0-6>*	Specify the maximum number of authentication retries.

Variable	Value
source-ip *WORD <0–46>*	Specify a configured IP address as the source address when transmitting RADIUS packets. RADIUS supports IPv4 and IPv6 addresses. WORD <0–46> specifies an address in A.B.C.D or x:x:x:x:x:x:x:x format.
timeout *<1-20>*	Specify the number of seconds before the authentication request times out.

Default

The default for used-by is CLI.

The default for acct-enable is enabled.

The default value for acct-port is 1816.

The default for priority is 10.

The default for retry is 3.

The default for timeout is 3.

Command mode

Global Configuration mode

radius-snmp acct-enable

Enable RADIUS accounting log all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Syntax

`radius-snmp acct-enable`

Parameters

Variable	Value
acct-enable	Enables RADIUS accounting globally. RADIUS accounting cannot be enabled unless a valid server is configured. This feature is disabled by default.

Default

The default value is disabled.

Command mode

Global Configuration mode

Related commands

Variable	Value
abort-session-timer <*30–65535*>	Specifies the timer to be used for sending a stop accounting message for this particular SNMP session. The timer value ranges from 30 to 65535. The default is 180.
re-auth-timer <*30–65535*>	Timer to be sent for re-authentication the SNMP session. The timer value ranges from 30 to 65535. The default is 180.
user *WORD<0–20>*	Specifies the user name for the SNMP access. *WORD<0–20>* specifies the user name in a range of 0 to 20 characters. The default is snmp_user.

radius sourceip-flag

Configure the source IP address if the outgoing interface on the Virtual Services Platform 9000 fails so that configuration changes be made to define the new RADIUS Client on the RADIUS Server.

Syntax

`radius sourceip-flag`

Parameters

None

Default

The default is disabled/false.

Command mode

Global Configuration mode

rlogin

Use this command to login remotely to a remote host.

Syntax

rlogin {A.B.C.D}

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address.

Default

None

Command mode

Privileged EXEC mode

rsh

Use this command to execute a shell command on a remote machine.

Syntax

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536> WORD<0-1536> WORD<0-1536>

rsh {A.B.C.D} -l WORD<0-1536> WORD<1-1536>

Parameters

Variable	Value
{A.B.C.D}	Specifies the IP address in the {A.B.C.D} format.
-l	User login name.

Variable	Value
WORD<0-1536>	Specifies the command to execute on the remote host: • Param1 for rsh command. String length {0–1536} • Param2 for rsh command. String length {0–1536} • Param3 for rsh command. String length {0–1536} • Param4 for rsh command. String length {0–1536} • Param5 for rsh command. String length {0–1536} • Param6 for rsh command. String length {0–1536} • Param7 for rsh command. String length {0–1536}

Default

None

Command mode

Privileged EXEC mode

show eapol auth-diags interface

Display the Extensible Authentication Protocol (EAPoL) Authenticator diagnostics to manage network performance.

Syntax

show eapol auth-diags interface

show eapol auth-diags interface gigabitethernet [{slot/port [-slot/port][,...]}]

show eapol auth-diags interface vlan <1–4084> [{slot/port [-slot/port][,...]}]

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan *<1–4084>*	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show eapol multihost-session-stats interface

Display the manage mode parameters for the specified interface type.

Syntax

show eapol multihost-session-stats interface

show eapol multihost-session-stats interface gigabitEthernet [{slot/port[-slot/port][,...]}]

show eapol multihost-session-stats interface vlan <1–4084>

show eapol multihost-session-stats interface vlan <1–4084> [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan <*1–4084*>	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show eapol port

Display Extensible Authentication Protocol (EAPoL) information for the specified port or interface type.

Syntax

show eapol port {slot/port [-slot/port][,...]}

show eapol port interface [gigabitEthernet {slot/port [-slot/port] [,...]}]

show eapol port interface gigabitEthernet

show eapol port interface vlan <1–4084> [{slot/port [-slot/port] [,...]}]

show eapol port interface vlan <1–4084>

Parameters

Variable	Value
gigabitethernet *{slot/port [-slot/port][,...]}*	Specifies the type of interface displayed.
vlan *<1–4084>*	Specifies the VLAN for which to show the statistics.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show eapol system

Display the current Extensible Authentication Protocol (EAPoL) setting on the switch.

Syntax

show eapol system

Parameters

None.

Default

None

Command mode

Privileged EXEC mode

show ip directed-broadcast

Shows the interface status for direct broadcast.

Syntax

`show ip directed-broadcast interface [GigabitEthernet]`

`show ip directed-broadcast interface GigabitEthernet [{slot/port}]`

Parameters

Variable	Value
{slot[-slot][,...]}	Identifies the slot in one of the following formats: a single slot (3), a range of slots (3-4), or a series of slots (3,5,6).

Default

None

Command mode

Privileged EXEC mode

show radius

Display the global status of RADIUS information.

Syntax

`show radius`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show radius-server

Display the RADIUS server information.

Syntax

show radius-server

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show radius-server statistics

Display current RADIUS server configurations.

Syntax

show radius-server statistics

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show radius snmp

Display the global status of RADIUS information.

Syntax

show radius snmp

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show snmp-server

Display Simple Network Management Protocol (SNMP) system information to view trap and authentication profiles.

Syntax

show snmp-server

show snmp-server community

show snmp-server context

show snmp-server group

show snmp-server host

show snmp-server notify-filter

show snmp-server user

show snmp-server view [viewname WORD<0–32>]

Parameters

Variable	Value
community	Displays the SNMP community table.
context	Displays vacm context table.
group	Displays SNMP group access table.
host	Displays SNMP host details.
notify-filter	Displays SNMP notify-filter details.
user	Displays SNMP users.
view	Displays SNMP MIB view table.
viewname *WORD<0–32>*	Displays the view for a particular view name.

Default

None

Command mode

Privileged EXEC mode

show snmp-server host

Display the SNMP server configuration information.

Syntax

show snmp-server host

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show snmp-server notify-filter

Display a new notify filter configuration information.

Syntax

show snmp-server notify-filter

Parameters

None

Default

None

Command mode

Privileged EXEC mode

snmp-server

Configure Simple Network Management Protocol (SNMP) to define or modify the SNMP settings, and specify how secure you want SNMP communications.

Syntax

`snmp-server`

Parameters

Variable	Value
agent-conformance enable	Activates agent conformance mode. Use the **`no`** operator to disable this configuration. To set this option to the default value, use the **`default`** operator with the command.
authentication-trap enable	Activates the generations of authentication traps. Use the **`no`** operator to disable this configuration. To set this option to the default value, use the **`default`** operator with the command.
bootstrap <min-secure| semi-secure| very-secure>	Creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (see RFC 3515, Appendix A). This command creates a set of initial users, groups, and views. • *min-secure*—a minimum security configuration that allows read access and notify access to all processes (MIB view restricted) with noAuth-noPriv and read, write, and notify access to all processes (MIB view internet) using Auth-Priv. In this configuration, restricted MIB view matches internet MIB view. • *semi-secure*—a security configuration that allows read access and notify access to all processes (MIB view restricted) with noAuth-noPriv and read, write, and notify access to all processes (MIB view internet) using Auth-Priv. In this configuration, restricted MIB view contains a smaller subset of views than internet MIB view. See RFC 3515 Appendix A for details. • *very-secure*—a maximum security configuration that allows no access to the users. Note that with this command all existing SNMP configurations in the SNMPv3 MIB tables are removed and replaced with entries as described in the RFC.

Variable	Value
community WORD<1–32> [group WORD <0–32>| index WORD<1–32>| secname WORD<1–32>] context WORD <0–32>	Sets the community table. • group WORD<0–32> specifies the group name in the range of 0 to 32 characters. • index WORD<1–32> specifies the community index in the range of 1 to 32 characters. • secname WORD <1–32> specifies the security name in the range of 1 to 32 characters. • context WORD <0–32> specifies the context name in the range of 0 to 32 characters.
contact *WORD<0-255>*	Changes the sysContact information for the switch. WORD<0-255> is an ASCII string from 0–255 characters (for example a phone extension or email address).
force-iphdr-sender enable	Configures the SNMP and IP sender flag to the same value. The default is disable. Use the **no** operator to remove this configuration. To set this option to the default value, use the **default** operator with the command.
force-trap-sender enable	Sends the configured source address (sender IP) as the sender network in the notification message. Use the **no** operator to remove this configuration. To set this option to the default value, use the **default** operator with the command.
login-success-trap enable	Enables the generation of login success traps.
location *WORD <0-255>*	Changes the sysLocation information for the switch. WORD <0-255> is an ASCII string from 0–255 characters.
name *WORD <0-255>*	Changes the sysName information for the switch. WORD<0-255> is an ASCII string from 0–255 characters.
sender-ip *<A.B.C.D> <A.B.C.D>*	Configures the SNMP trap receiver and source IP addresses. Specify the IP address of the destination SNMP server that will receive the SNMP trap notification in the first IP address. Specify the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If this is set to 0.0.0.0 then the switch uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

Default

None

Command mode

Global Configuration mode

snmp-server community

Create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers.

Syntax

snmp-server community WORD<1–32> [group WORD<0–32>] [index WORD<1–32>] [secname WORD<1–32>] [context WORD<0–32>]

Parameters

Variable	Value
group *WORD<0–32>*	Specifies the group name. The range is 0–32 characters.
index *WORD<0–32>*	Specifies the unique index value of a row in this table. The range is 0–32 characters.
WORD<1–32>	Specifies a community string, from 1–32 characters.
secname *WORD<0–32>*	Maps the community string to the security name in the VACM Group Member Table. The range is 0–32 characters.
context *WORD<0–32>*	Specifies the context name. The range is 0–32 characters.

Default

None

Command mode

Global Configuration mode

snmp-server group

Create a new user group member to logically group users who require the same level of access.

Syntax

snmp-server group WORD<1–32> WORD<0–32> [auth-no-priv|auth-priv|no-auth-no-priv] [notify-view WORD <0–32>] [read-view WORD<0–32>] [write-view WORD<0–32>]

Parameters

Variable	Value
auth-no-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the **auth-no-priv** parameter is included, it creates one entry for SNMPv3 access.
auth-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the **auth-priv** parameter is included, it creates one entry for SNMPv3 access.
WORD<0–32>	Creates a group entry for a particular context. The range is 0–32 characters. If you use a particular group name value but with different context names, you create multiple entries for different contexts for the same group. You can omit the context name and use the default. If the context name value ends in the wildcard character (*), the resulting entries match a context name that begins with that context. For example, a context name value of foo* matches contexts starting with foo, such as foo6 and foofofum. Use the **no** operator to remove this configuration.
group *WORD<1–32>*	Assigns the group name for data access. The range is 1–32 characters. Use the **no** operator to remove this configuration.
no-auth-no-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the **no-auth-no-priv** parameter is included, it creates 3 entries, one for SNMPv1 access, one for SNMPv2c access, and one for SNMPv3 access.
notify-view *WORD<0–32>*	Specifies the view name in the range of 0–32 characters.
read-view *WORD<0–32>*	Specifies the view name in the range of 0–32 characters.
write-view *WORD<0–32>*	Specifies the view name in the range of 0–32 characters.

Default

None

Command mode

Global Configuration mode

snmp-server user

Create a user on the local system in the USM table to authorize a user on a particular SNMP engine.

Syntax

snmp-server user WORD<1–32> [read-view WORD<0–32>] [write-view WORD<0–32>] [notify-view WORD<0–32>] [{md5|sha} <password>] [{aes|des} <password>

Parameters

Variable	Value
{aes|des} *WORD<1–32>*	Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes or des. **<WORD 1–32>** assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters. **Important:** You must set authentication before you can set the privacy option.
{md5|sha} *WORD<1–32>*	Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are MD5 and SHA. **<WORD 1–32>** specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1–32 characters.
notify-view *WORD<0–32>*	Specifies the view name in the range of 0-32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
read-view *WORD <0–32>*	Specifies the view name in the range of 0-32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
write-view *WORD<0–32>*	Specifies the view name in the range of 0-32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
user*WORD<1–32>*	Creates the new entry with this security name. The name is used as an index to the table. The range is 1–

Variable	Value
	32 characters. Use the **no** operator to remove this configuration.

Default

None

Command mode

Global Configuration mode

snmp-server user engine-id

Create a new user on the remote system in the USM table to authorize a user on a particular SNMP engine.

Syntax

snmp-server user engine-id WORD<16-97> WORD<1-32>

snmp-server user engine-id WORD<16-97> WORD<1-32> {md5|sha} WORD<1-32>

snmp-server user engine-id WORD<16-97> WORD<1-32> {md5|sha} WORD<1-32> [{aes|des} WORD <1-32>]

Parameters

Variable	Value
{aes|des} *WORD<1-32>*	Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes or des. **WORD 1-32** assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters.
engine-id *WORD<16-97>*	Assigns an SNMPv3 engine ID. The range is 16 to 97 characters. Use the **no** operator to remove this configuration.
{md5|sha} *WORD<0–32>*	Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are MD5 and SHA. **password** specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1–32 characters.

Default

None

Command mode

Global Configuration mode

snmp-server user group

Add the user to a group to authorize a user on a particular SNMP engine.

Syntax

snmp-server user WORD <1–32> group WORD <1–32> [{md5|sha} WORD <1–32>]

snmp-server user WORD <1–32> group WORD <1–32> {md5|sha} WORD <1–32> [{aes|des} WORD <1–32>]

snmp-server user WORD <1–32> group WORD <1–32>

Parameters

Variable	Value
{aes|des} *WORD <1–32>*	Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes or des. **WORD <1–32>** assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters. **Important:** You must set authentication before you can set the privacy option.
group *WORD <1–32>*	Specifies the group access name.
{md5|sha} *WORD <1–32>*	Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are MD5 and SHA. **password** specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1–32 characters.
user*WORD <1–32>*	Creates the new entry with this security name. The name is used as an index to the table. The range is 1–32 characters. Use the **no** operator to remove this configuration.

Default

None

Command mode

Global Configuration mode

snmp-server view

Create a new entry in the MIB view table. The default Layer 2 MIB view cannot modify SNMP settings. However, a new MIB view created with Layer 2 permission can modify SNMP settings.

Syntax

snmp-server view WORD <1–32> WORD <1–32>

Parameters

Variable	Value
WORD <1–32>	Specifies the prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1–32 characters.
WORD <1–32>	Specifies a new entry with this group name. The range is 1–32 characters.

Default

None

Command mode

Global Configuration mode

snmp trap link-status

Enable link trap on the port.

Syntax

snmp trap link-status [port {slot/port[-slot/port][,...]}] enable

default snmp trap link-status [port {slot/port[-slot/port][,...]}] enable

no snmp trap link-status [port {slot/port[-slot/port][,...]}] enable

Parameters

Variable	Value
enable	Enables or disables link-trap status for the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is enabled.

Command mode

GigabitEthernet Interface Configuration mode

Chapter 16: Troubleshooting commands

This chapter describes the Avaya Command Line Interface (ACLI) commands to help you troubleshoot the Avaya Virtual Services Platform 9000.

action flushArp

Flush or clear the Address Resolution Protocol (ARP) tables for administrative and troubleshooting purposes.

Syntax

action [none|flushMacFdb|flushArp|flushIp|triggerripupdate|flushAll|clearLoopDetectAlarm]

action port {slot/port [-slot/port][,...]} [none|flushMacFdb|flushArp|flushIp|triggerripupdate|flushAll|clearLoopDetectAlarm]

Parameters

Variable	Value
port *{slot/port [-slot/port][,...]}*	Specifies the slot and the port list that needs to be changed.
none	Sets action to none.
flushMacFdb	Sets action to flushMacFdb.
flushArp	Sets action to flushArp.
flushIp	Sets action to flushIp.
triggerRipUpdate	Sets action to triggerRipUpdate.
flushAll	Sets action to flush all.
ClearLoopDetectAlarm	Sets action to clear loop detect alarm.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

action flushIp

Flush or clear the routing tables for administrative and troubleshooting purposes.

Syntax

`action flushIp`

Parameters

none

Default

None

Command mode

GigabitEthernet Interface Configuration mode

action flushMacFdb

Flush or clear the MAC address tables for administrative and troubleshooting purposes.

Syntax

`action flushMacFdb`

Parameters

none

Default

None

Command mode

GigabitEthernet Interface Configuration mode

boot config logfile

Configure logfile parameters. The log file is named using an 8.3 (xxxxxxxx.sss) format. The first six characters of the file name contain the last three bytes of the chassis base MAC address. The next two characters specify the slot number of the CP module that generated the logs. The last three characters denote the sequence number of the log file. Multiple sequence numbers are generated for the same chassis and same slot, if you replace or reinsert the CP module, or if the maximum log file size is reached.

Syntax

boot config logfile <64–500> <500–16384> <10–90>

default boot config logfile

Parameters

Variable	Value
<64–500>	Specifies the minimum free memory space on the external storage device from 64– 500 KB. Virtual Services Platform 9000 does not support this parameter.
<500–16384>	Specifies the maximum size of the log file from 500–16384 KB.
<10–90>	Specifies the maximum percentage, from 10–90%, of space on the external storage device the log file can use. Virtual Services Platform 9000 does not support this parameter.

Default

None

Command mode

Global Configuration mode

clear ip arp interface

Clear the ARP timers.

Syntax

clear ip arp interface gigabitethernet {slot/port[-slot/port][,...]}

clear ip arp interface vlan <1–4084>

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

clear ip route

Clear the routing table.

Syntax

clear ip route [gigabitethernet {slot/port}|vlan <1-4084>]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

clear ip vrrp

Clear the Virtual Router Redundancy Protocol (VRRP) configuration.

Syntax

clear ip vrrp vlan <1-4084> vrid <1–255>

clear ip vrrp gigabitethernet {slot/port[-slot/port][,...]} vrid <1–255>

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID.
<1–255>	Specifies the ID of the virtual router.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

clilog

Use ACLI logging to track all ACLI commands executed and for fault management purposes. The ACLI commands are logged to the system log file as CLILOG module.

Syntax

`clilog enable`

`default clilog enable`

`no clilog enable`

Parameters

Default

The default is disabled.

Command mode

Global Configuration mode

debug ip pim

Use PIM traces to aid in PIM troubleshooting.

Syntax

`debug ip pim pimdbgtrace`

Parameters

Variable	Value
pimdbgtrace	Enables or disables PIM debug traces.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
assert	Sets the assert debug traces to true.
bstrap	Sets bootstrap debug traces to true.
group *<A.B.C.D>*	Sets the group value to a specific multicast group value from a specific group IP address.
hello	Sets hello debug trace to true.
join-prune	Sets join/prune debug trace to true.
pimdbglog	Enables whether the switch logs debug traces.
rcv-dbg-trace	Sets trace messages received by the switch to true.
register	Sets register debug trace to true.
regstop	Sets register stop debug trace to true.
rp-adv	Sets RP advertisement debug trace to true.
send-dbg-trace	Sets send trace messages forwarded by the switch to true.
source *<A.B.C.D>*	Sets debug traces from a specific source IP address to true.

dump ar

To aid in troubleshooting, a dump of the hardware records can be captured.

Syntax

`dump ar <1–12> WORD<1-1536> <0-3>`

Parameters

Variable	Value
<1–12>	Specifies the slot number from 1 to 12.
WORD<1-1536>	Specifies a record type in the AR table. Options include vlan, ip_subnet, mac_vlan, mac, arp, ip, ipmc, ip_filter, protocol, all.
<0-3>	Specifies the verbosity from 0 to 3. Higher numbers specify more verbosity.

Default

None

Command mode

Privileged EXEC mode

exception dump

Configure and enable the core-file collection on the switch.

Syntax

`exception dump {slot [-slot][,...]} enable`

Parameters

Variable	Value
{slot [-slot][,...]}	Specifies the slot list to enable the core-files on the switch. Valid slots are 1 to 12, SF1 to SF6, or all.
core-pattern *WORD <1–32>*	Denotes the pattern for generating core-file names.
directory*WORD <1–64>*	Specifies the directory to store core-files. *WORD <1–64>* specifies the name of the directory file to be stored in the range of 1 to 64 characters.
enable	Enables the core-file collection on the slots specified.
max-disk-space*<100–1024>*	Maximum disk space (in MB) allocated for the collection of core-files.

Default

None

Command mode

Global Configuration mode

extflash-stop

Use this command to safely remove the external Compact Flash device.

Syntax

`extflash-stop`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

fabric statistics

Enable fabric statistics on the given port.

Syntax

`fabric statistics [port {slot/port [-slot/port][,...]}] [enable]`

Parameters

Variable	Value
enable	Enables fabric statistics on the port specified.
port *{slot/port [-slot/port][,...]}*	Specifies the port number that needs to be changed.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

flight-recorder

Perform various functions on the flight recorder data on the switch.

Syntax

`flight-recorder all {slot [-slot][,...]}`

`flight-recorder archive {slot [-slot][,...]}`

flight-recorder snapshot {slot [-slot][,...]}

flight-recorder trace {slot [-slot][,...]}

Parameters

Variable	Value
all *{slot [-slot][,...]}*	Creates flight recorder snapshot, trace, and archive. *{slot [-slot][,...]}* specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
archive *{slot [-slot][,...]}*	Creates tarball of flight recorder files, log files, config file and others. *{slot [-slot][,...]}* specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
snapshot *{slot [-slot][,...]}*	Takes the snapshot of flight recorder PMEM data. *{slot [-slot][,...]}* specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.
trace *{slot [-slot][,...]}*	Takes the snapshot of always-on-trace data. *{slot [-slot][,...]}* specifies the slot number. Valid slots are 1 to 12, SF1 to SF6, or all.

Default

None

Command mode

Privileged EXEC mode

global-debug mask

Display specific debug messages for your global BGP configuration.

Syntax

global-debug mask WORD <1-100>

default global-debug mask

no global-debug mask

Parameters

Variable	Value
mask *WORD <1-100>*	Specifies one or more mask choices that you enter, separated by commas with no space between choices. For example, [<mask>,<mask>,<mask>...]. Options include: none, all, error, packet, event, trace, warning, state, init, filter, update.

Default

None

Command mode

BGP Router Configuration mode

grep

Use this Unix command to search files for lines that match a given expression.

Syntax

`grep WORD<0–1536>`

`grep error WORD<1–99>`

Parameters

Variable	Value
grep *WORD <0–1536>*	Searches files for lines that match a given expression. WORD<0–1536> specifies the string to match.
grep error *WORD <0–99>*	Search for an error in a file. *WORD<1–99>* specifies a filename, /intflash/<file>, /extflash/<file>, /usb/<file>.

Default

None

Command mode

Privileged EXEC mode

line-card level

Perform trace commands for input/output and switch fabric cards.

Syntax

`line-card [<3–12>|SF1|SF2|SF3|SF4|SF5|SF6] trace [level <67–92>] [grep <WORD <0–1024>]`

Parameters

Variable	Value
<3–12>	Specifies the slot number for IO card in the range of 3 to 12.
SF1	Switch Fabric 1.
SF2	Switch Fabric 2.
SF3	Switch Fabric 3.
SF4	Switch Fabric 4.
SF5	Switch Fabric 5.
SF6	Switch Fabric 6.
level *<67–92>*	Sets the trace level.
grep *<0–1024>*	Greps the string in the range of 0 to 1024.
trace	Sets the trace level.

Default

None

Command mode

Privileged EXEC mode

logging level

Determine what messages the system records in the log.

Syntax

`logging level <0-4>`

Parameters

Variable	Value
`level <0-4>`	Shows and configures the logging level. The level is one of the following values: 0 = Information; all messages are recorded. 1 = Warning; only warning and more serious messages are recorded. 2 = Error; only error and more serious messages are recorded. 3 = Manufacturing; this parameter is not available for customer use. 4 = Fatal; only fatal messages are recorded.

Default

None

Command mode

Global Configuration mode

logging logToExtFlash

Begin or stop logging system messages to the external flash.

Syntax

`logging logToExtFlash`

`no logging logToExtFlash`

`default logging logToExtFlash`

Parameters

None

Default

The default is **`no logging logToExtFlash`**, which indicates the system logs messages to the external flash.

Command mode

Global Configuration mode

logging screen

Configure the system to display log messages on screen.

Syntax

`logging screen`

Parameters

Variable	Value
`screen`	Configures the system to display the log messages on screen.

Default

None

Command mode

Global Configuration mode

logging transferFile

Configure the remote host address for log transfer. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

Syntax

`logging transferFile <1-10> address <A.B.C.D>`

Parameters

Variable	Value
`<1–10>`	Specifies the file ID to transfer.
`address <A.B.C.D>`	Specifies the IP address of the host to which to transfer the log file. The remote host must be reachable or the configuration fails.

Default

None

Command mode

Global Configuration mode

logging transferFile filename-prefix

Create the filename on the remote host. The system transfers the current log file to a remote host when the log file size reaches the configured maximum size.

Syntax

logging transferFile <1-10> filename-prefix WORD<0–200>

Parameters

Variable	Value
<1–10>	Specifies the file ID to transfer.
filename–prefix WORD<0-2005>	Specify the name of the file on the remote host. If you do not configure a name, the current log file name is the default. **Important:** Avaya recommends that you do not configure this option. If you configure this option, the previously transferred log file is overwritten on the remote server.

Default

None

Command mode

Global Configuration mode

logging write

Write to the log file automatically created by the system.

Syntax

logging write WORD<1-1536>

Parameters

Variable	Value
write WORD<1-1536>	Writes the designated string to the log file. WORD<1-1536>

Variable	Value
	is the string or command that you append to the log file. If the string contains spaces, you must enclose the string in quotation marks (").

Default

None

Command mode

Global Configuration mode

mirror-by-port

Use port mirroring to aid in diagnostic and security operations.

Syntax

mirror-by-port <1-479> in-port {slot/port [slot/port][,...]} {monitor-ip {A.B.C.D} [dscp <0-63>][enable] [mode<both|tx|rx>] [ttl<2–255>] | monitor-mlt <1-512>|monitor-vlan <1-4084>|out-port {slot/port [slot/port][,...]}}

mirror-by-port <1-479> [enable] [mode<both|tx|rx>] [remote-mirror-vlan-id<1-4084>]

default mirror-by-port <1-479> [enable] [mode] [remote-mirror-vlan-id]

default mirror-by-port mirror-port <1-479> {slot/port[-slot/port][,...]}

default mirror-by-port monitor-ip <1-479> {A.B.C.D} [dscp][ttl]

default mirror-by-port monitor-mlt <1-479> <1–512>

default mirror-by-port monitor-port <1-479> {slot/port[-slot/port][,...]}

default mirror-by-port monitor-vlan <1-479> <1–4084>

no mirror-by-port <1-479> [enable]

no mirror-by-port mirror-port <1-479> {slot/port[-slot/port][,...]}

no mirror-by-port monitor-ip <1-479> {A.B.C.D}

no mirror-by-port monitor-mlt <1-479> <1–512>

no mirror-by-port monitor-port <1-479> {slot/port[-slot/port][,...]}

no mirror-by-port monitor-vlan <1-479> <1–4084>

Parameters

Variable	Value
<1-479>	Specifies the mirror-by-port entry ID in the range of 1 to 479.
enable	Enables or disables a mirroring instance already created in the mirror-by-port table.
[in-port *{slot/port [slot/port][,...]}* {monitorip {A.B.C.D} [dscp *<0-63>*] [*<2-255>*]|monitor-mlt *<1-512>*|monitor-vlan *<1-4084>*|out-port *{slot/port [slot/port][,...]}*}]	Creates a new mirror-by-port table entry. • in-port {slot/port [slot/port][,...]} specifies the mirrored port. • monitor-ip {A.B.C.D} [dscp <0-63>] [<2-255> specifies the destination IP address for Layer 3 remote mirroring. You can optionally configure the DSCP and time-to-live values, or accept the defaults. • monitor-mlt <1-512> specifies the mirroring MLT ID from 1 to 512. • monitor-vlan <1–4084> specifies the mirroring VLAN ID from 1 to 4084. • out-port {slot/port [slot/port][,...]} specifies the mirroring port.
mirror-port *<1-479> {slot/port [slot/port][,...]}*	Modifies the mirrored port. Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable`.
monitor-ip *<1-479>* {A.B.C.D} [dscp <0-63>] [*<2-255>*][ttl*<2–255>*]	Creates a mirroring instance for Layer 3 remote mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 0 and the default is 64. TTL sets the time-to-live value between 2 to 255 seconds.
monitor-mlt *<1-479> <1-512>*	Modifies the monitoring MLT; *<1–479> <1-512>* specifies the port mirroring entry id and the MLT ID. Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable` .
monitor-port *<1-479> {slot/port [slot/port] [,...]}*	Modifies the monitoring ports. Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable` .
monitor-vlan *<1-479> <1-4084>*	Modifies the monitoring VLAN.

Variable	Value
	Before you can modify an existing entry, you must disable the entry: `no mirror-by-port <1-479> enable`.
mode <both|tx|rx>	Sets the mirroring mode. The default is rx. • *both* mirrors both egress and ingress packets. • *tx* mirrors egress packets. • *rx* mirrors ingress packets.
remote-mirror-vlan-id *<1-4084>*	Sets the remote mirror VLAN ID.

Default

The default DSCP is 0. The default TTL is 64.

Command mode

Global Configuration mode

neighbor-debug-all

Displays specified debug information for BGP neighbors.

Syntax

`neighbor-debug-all mask <WORD 1-100>`

`default neighbor-debug-all`

`no neighbor-debug-all`

Parameters

Variable	Value
mask <*WORD 1-100*>	<*WORD 1-100*> is a list of mask choices separated by commas with no space between choices.

Default

The default value is none.

Command mode

BGP Router Configuration mode

pcap capture-filter

Use capture filters to better define the match criteria used on packets.

Avaya highly recommends using PCAP with IP or MAC filters to reduce the load on the PCAP engine.

Syntax

pcap capture-filter <1-1000>

Parameters

Variable	Value
action <capture|drop|trigger-on|trigger-off>	Determines the action taken by the filter. • **capture** indicates that the packet is captured. • **drop** indicates that the packet is dropped. • **trigger-on** indicates to start capturing the packet when a packet matches this filter. PCAP is enabled globally and the trigger filter is disabled. • **trigger-off** indicates to stop capturing the packet when a packet matches this filter. PCAP is disabled globally and the trigger filter is disabled.
dscp *<0-63> [<0-63>]* [match-zero]	Specifies the DSCP value of the packet. **<0-63>** is the DSCP from 0 to 63. The default is 0, which means this option is disabled. Use the second **<0-63>** to specify a range. When **match-zero** is set, 0 is considered a valid value. When it is not set, 0 is considered a disable value.
dstip *<A.B.C.D> [<A.B.C.D>]*	Specifies the destination IP address. The default is 0.0.0.0, which means this option is disabled. Use the second **<A.B.C.D>** to specify a range.
dstmac *<0x00:0x00:0x00:0x00:0x00:0x00> [<1-6>]*	Specifies the MAC address of the destination. If the mask is set, then only the first few bytes are compared. **<1-6>** is the destination MAC address mask, and specifies a range.
enable	Enables the filter. The default is disable.
ether-type *<0x0-0xffff> [<0x0-0xffff>]*	Specifies the Ethernet type of the packet. **<Ethertype>** is an Ether-type. The default is 0, meaning that this option is disabled.

Variable	Value
	Use the second **<0x0-0xffff>** to specify a range.
packet-count <*0-65535*>	When set, PCAP stops after capturing the specified number of packets. This is similar to the refresh-timer option; after it is invoked, the filter is disabled. This option is active only when the action parameter is set to trigger-on. The default value is 0, which means this option is disabled.
pbits <*0-7*> <*0-7*>[match-zero]	Specifies the priority bit of the packet. The default is 0, which means this option is disabled. Use the second **<0-7>** to specify a range. When **match-zero** is set, 0 is considered a valid value. When it is not set, 0 is considered a disable value.
protocol-type <*0-255*> *[<0-255>]*	Specifies the packet protocol type. The default is 0, which means this option is disabled. Use the second **<0-255>** to specify a range.
refresh-timer <*WORD 1-7*>	When set, this starts or resets a timer. If another packet is not received within the specified time, PCAP is disabled globally. This option is active only when the action parameter is set to 'trigger-on'. To delete this option, set it to 0. The default value is 0.
srcip <*A.B.C.D*> *[<A.B.C.D>]*	Specifies the source IP address. The default is 0.0.0.0, which means this option is disabled. Use the second **<A.B.C.D>** to specify a range.
srcmac <*0x00:0x00:0x00:0x00:0x00:0x00*> *[<1-6>]*	Specifies the MAC address of the source. If the mask is set, then only the first few bytes are compared. The default is 00:00:00:00:00:00, which means this option is disabled. **<1-6>** is the mask of the source MAC address. This parameter specifies an address range.
tcp-port <*0-65535*> *[<0-65535>]*	Specifies the TCP port of the packet. The default is 0, which means this option is disabled. Use the second **<0-65535>** to specify a range.
timer <*WORD 1-7*>	When set, PCAP is invoked when the first packet is matched and stopped after the set value of time. After starting the timer, the filter is disabled. This option is active only when the action parameter is set to trigger-on. **<WORD 1-7>** is a value from 100 to 3600000 milliseconds. The default value is zero. Setting the value to 0 disables the timer.
udp-port <*0-65535*> *[<0-65535>]*	Specifies the UDP port of the packet.

Variable	Value
	The default is 0, which means this option is disabled. Use the second **<0-65535>** to specify a range.
user-defined <*0-9600*> <*WORD 0-50*>	Sets a user defined value on which to match the packet. The user can define a pattern in hex or characters to match (**<0-9600>**). The user can also specify the offset to start the match (**<WORD 0-50>**). The default value of pattern is null ('') which means that this field is discarded. To disable this option, set the pattern to null ('').
vid <*1-4084*> *[<1-4084>]*	Specifies the VLAN ID of the packet. The default is 0, which means that this option is disabled. Use the second **<1-4084>** to specify a range.

Default

None

Command mode

Global Configuration mode

pcap enable

Configure PCAP globally to define how PCAP operates on the Virtual Services Platform 9000.

Syntax

pcap enable

Parameters

Variable	Value
auto-save [file-name <*WORD 1-40*>| extflash| network <*A.B.C.D*>]	Enables or disables auto save. When enabled, saves the captured frames into the device specified and continues to capture frames. The default is enable. If this option is disabled, packets are stored in the DRAM buffer only. **file-name <WORD 1-40>** is the name of the file where captured frames are saved. **extflash** sets the device to external flash. **network** sets the device to network. **<A.B.C.D>** is the IP address used. This is used only if the device is network.

Variable	Value
buffer-size *<2-128>*	Specifies the size of the buffer allocated for storing data.
buffer-wrap	Enables buffer wrapping. When this parameter is set to true and the buffer becomes full, the capture continues by wrapping the buffer. If this parameter is set to false and the buffer becomes full, the packet capture stops. The default value is true. A log message is generated when the buffer is wrapped.
enable	Enables PCAP globally. The default is disabled. To disable PCAP, use the **`no pcap enable`** command.
fragment-size *<64-9600>*	Specifies the number of bytes from each frame to capture. The default is the first 64 bytes of each frame.
reset-stat	This command resets the PCAP engine DRAM buffer, as well as all software counters used for PCAP statistics. This command can be executed in the Primary or Secondary CPU.
wrap-auto-save-file	Enables wrap around auto-save-file (external flash—wrap around).

Default

None

Command mode

Global Configuration mode

pcap enable mode

Enable PCAP globally.

Syntax

`pcap enable mode <tx|rx|both>`

Parameters

None

Default

None

Command mode

GigabitEthernet Interface Configuration mode

pcap reset-stat

Reset PCAP statistics and counters.

Syntax

pcap reset-stat

Parameters

None

Default

None

Command mode

Global Configuration mode

ping

Ping a device to test the connection between the Avaya Virtual Services Platform 9000 and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears that indicates traffic can reach the specified IP address. If the switch does not receive a reply, the message indicates the address is not responding.

Syntax

ping WORD<0–256> [-d] [-I <1–60>] [-s] [-t <1–120>] [count <1–9999>] [datasize <16–51200>] [interface WORD <1–256>|gigabitEthernet| mgmtEthernetport|tunnel|vlan] [source WORD <1–256>] [scopeid <1–9999>] [vrf WORD<0–16>]

Parameters

Variable	Value
count *<1–9999>*	Specifies the number of times to ping (for IPv4) (1–9999).
-d	Configures the ping debug mode. This variable detects local software failures (ping related threads creation or write to sending socket) and receiving issues (icmp packet too short or wrong icmp packet type).

Variable	Value
datasize *<16–65487>*	Specifies the size of ping data sent in bytes (for IPv4) (16–65487).
interface {WORD <1–256>[gigabitEthernet|mgmtEthernet|tunnel|vlan]}	Specifies a specific outgoing interface to use by IP address. Additional ping interface filters: • gigabitEthernet: {slot/port} gigabit ethernet port • mgmtEthernetport: {slot/port} management ethernet port • tunnel: tunnel ID as a value from 1 to 2147477248 • vlan: VLAN interface as a value from 1 to 4084
-I *<1–60>*	Specifies the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the [-I] parameter (for IPv4).
scopeid *<1–9999>*	Specifies the scope ID. *<1–9999>* specifies the circuit ID for IPv6.
source WORD *<1–256>*	Specifies an IP address that will be used as the source IP address in the packet header.
-t *<1–120>*	Specifies the no-answer timeout value in seconds (1–120) for IPv4.
vrf *WORD <0–16>*	Specifies the virtual router and forwarder (VRF) name from 1–16 characters. Specify the MgmtRouter VRF if you need to run the ping operation through the management interface.
WORD *<0–256>*	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address (string length 0–256). Specifies the address to ping.

Default

None

Command mode

Privileged EXEC mode

remote-mirroring

Use remote mirroring to monitor many ports from different switches using one network probe device.

Syntax

remote-mirroring [enable] [mode <source|termination>] [port {slot/port [-slot/port][,...][,...]}] [srcMac <0x00:0x00:0x00:0x00:0x00:0x00>] [dstMac <0x00:0x00:0x00:0x00:0x00:0x00>] [ether-type <0x00-0xffff>] [vlan-id <1-4084>]

Parameters

Variable	Value
dstMac *<0x00:0x00:0x00:0x00:0x00:0x00>*	Sets the destination MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent to this MAC address. The DstMac is used only for RMS ports. For RMT ports, one of the unused MAC addresses from the switch port MAC address range is used. This MAC address is saved in the configuration file.
enable	Enables remote mirroring on the port. When remote mirroring is enabled, the following events occur: • A static entry for the DstMac is added to the Forwarding Database (FDB). All packets that come with this remote mirroring DstMac are sent to the RMT port. • The switch periodically (once in 10 seconds) transmits broadcast Layer 2 packets in the associated VLAN so that all nodes in the network can learn the DstMac.
ether-type *<0x00-0xffff>*	Specifies the Ethertype of the remote mirrored packet. The default value is 0x8103.
mode <source|termination>	Specifies whether the port is an RMT (mode is termination) or an RMS (mode is source).
srcMac *<0x00:0x00:0x00:0x00:0x00:0x00>*	Sets the source MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent from the RMS port, and the source MAC parameter in the header is derived from this address. The source MAC

Variable	Value
	address of the encapsulated frame contains the first 45 bits of this MAC address. The three least significant bits are derived from the port number of the RMS port. The MAC address of the port is used as the default value.
vlan-id *<1-4084>*	Specifies to which VLAN the remote mirroring destination MAC address belongs. This must be a port-based VLAN. Used only for Remote Mirroring Termination (RMT) ports. When the RMT port is removed from the last VLAN in the list, RMT is disabled on the port.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

save clilog

Saves the CLI logs to a file.

Note:

The following command is only applicable to log files generated by past releases prior to Release 3.2. This command is obsolete starting with Release 3.2.

Syntax

`save clilog [file WORD<1–99>]`

Parameters

Variable	Value
file *WORD<1–99>*	Specifies the file name in one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file>

Variable	Value
	/mnt/intflash is equivalent to the /intflash of the standby CP (if present). /mnt/extflash is equivalent to the /extflash of the standby CP (if present). *WORD<1–99>* is a string of 1–99 characters.

Default

None

Command mode

Privileged EXEC mode

save log

Saves the log files, assuming the files use the default file names.

Syntax

`save log [file WORD<1-99>]`

Parameters

Variable	Value
file *WORD<1–99>*	Specifies the file name in one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *WORD<1–99>* is a string of 1–99 characters.

Default

None

Command mode

Privileged EXEC mode

save snmplog

Save the SNMP trap log files to a file.

Note:

The following command is only applicable to log files generated by past releases prior to Release 3.2. This command is obsolete starting with Release 3.2.

Syntax

`save snmplog [file WORD<1–99>]`

Parameters

Variable	Value
file *WORD<1–99>*	Specifies the file name in one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *WORD<1–99>* is a string of 1–99 characters.

Default

None

Command mode

Privileged EXEC mode

save trace

Save the trace file to the card for retrieval.

Syntax

`save trace [file WORD<1-99>]`

Parameters

Variable	Value
file *WORD<1-99>*	Specifies the file name in one of the following formats: • a.b.c.d: <file> • /intflash/ <file> • /extflash/ <file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> • /usb/<file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) . /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) .

Default

None

Command mode

Privileged EXEC mode

show clilog

Verify the configuration and view the log file.

Note:

The following command is only applicable to log files generated by past releases prior to Release 3.2. The command is replaced by `show logging file module clilog` for new files.

Syntax

`show clilog [file] [tail] [grep WORD<1-256>]`

Parameters

Variable	Value
file	Shows the log file.
grep *WORD <1-256>*	Shows the last results first.
tail	Performs a string search in the log file. *WORD <1-256>* is the string, of up to 256 characters in length, to match.

Default

None

Command mode

Privileged EXEC mode

show core-files

Displays the core files generated by the exception dump command.

Syntax

`show core-files {slot [-slot][,...]}`

Parameters

Variable	Value
{slot [-slot][,...]}	Specifies the slot number to display the core files. Valid slots are 1 to 12, SF1 to SF6, and all.

Default

None

Command mode

Privileged EXEC mode

show fabric

Displays complete fabric information on the switch.

Syntax

show fabric [cp <1–2>|io <3–12>|sf <SF1|SF2|SF3|SF4|SF5|SF6>statistics cos <0–7>]

Parameters

Variable	Value
cp *<1–2>*	Displays fabric information for the CP card. *<1–2>* specifies the CP slot number.
io *<3–12>*	Displays fabric information for the IO card. *<3–12>* specifies the IO slot number.
sf <SF1|SF2|SF3|SF4|SF5|SF6>	Displays fabric information for the SF card.
statistics cos *<0–7>*	Displays the fabric statistics. *<0–7>* specifies the cos ID.

Default

None

Command mode

Privileged EXEC mode

show logging

Use this command to display logging information.

Syntax

show logging info

show logging config

show logging level

show logging transferFile <1–10>

Parameters

Variable	Value
config	Displays the global logging information.
info	Displays the logging information.
level	Displays the configuration of event logging.
transferFile <1–10>	Displays the current level parameter settings and next level directories. <*1–10*> specifies the TFTP/FTP host IP address.

Default

None

Command mode

Privileged EXEC mode

show logging file

View log files by file name, category, severity, or CP module to identify possible problems.

Syntax

`show logging file [alarm][CPU WORD<0-25>] [event-code WORD<0–10>}] [module WORD<0–100>] [name-of-file WORD<1-99>] [save-to-file WORD<1-99>] [severity WORD<0-25>] [tail] [vrf WORD<0–32>]`

Parameters

Variable	Value
alarm	Displays alarm log entries.
CPU *WORD <0-25>*	Filters and list the logs according to the CP module that generated it. Specify a string length of 0–25 characters. To specify multiple filters, separate each CP module by the vertical bar (|), for example, CPU1|CPU2.
event-code *WORD<0–10>*	Specifies a number that precisely identifies the event reported. *WORD<0–10>* specifies the event code in the format: {0x0-0x00FFFFFF| 0x0-0x00FFFFFF}.
module <*WORD 0-100*>	Filters and list the logs according to module. Specify a string length of 0–100 characters. Categories include SNMP, EAP, RADIUS, RMON, WEB, STG, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP, and SNMPLOG. To specify multiple filters,

Variable	Value
	separate each category by the vertical bar (|), for example, OSPF|FILTER|QOS. Use the command `show logging file module clilog` to view the ACLI log. Use the command `show logging file module snmplog` to view the SNMP log.
name-of-file *WORD <1-99>*	Displays the valid logs from this file. For example, /intflash/logcopy.txt. You cannot use this command on the current log file—the file into which the messages are currently logged). Specify a string length of 1–99 characters.
save-to-file *WORD <1-99>*	Redirects the output to the specified file and removes all encrypted information. The tail option is not supported with the save-to-file option. Specify a string length of 1–99 characters. The format for the file name is: • /intflash/<file> • /extflash/<file> • /usb/<file> • /mnt/intflahs/<file> • /mnt/extflash/<file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *Word<1–99>* is a string of 1–99 characters.
severity *WORD <0-25>*	Filters and list the logs according to severity. Choices include INFO, ERROR, WARNING, FATAL. To specify multiple filters, separate each severity by the vertical bar (|), for example, ERROR|WARNING|FATAL.
tail	Shows the last results first.
vrf *WORD<0–32>*	Specifies the name of a VRF instance to show log messages that only pertain to that VRF.

Default

None

Command mode

Privileged EXEC mode

show pcap

Display PCAP information.

Syntax

show pcap

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show pcap capture-filter

Display packet capture (PCAP) filter configurations.

Syntax

show pcap capture-filter <1–1000>

Parameters

Variable	Value
<1–10>	Specifies the capture filter ID.

Default

None

Command mode

Privileged EXEC mode

show pcap dump

You can view packets using a ACLI session and the Secondary CPU. Dumping a large number of captured packets is CPU intensive. The switch does not respond to any commands while

the dump is in progress. Avaya recommends you use this command only when it is absolutely necessary. However, there is no degradation in normal traffic handling or switch failover.

Syntax

show pcap dump

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show pcap port

Display PCAP port information to ensure accuracy.

Syntax

show pcap port

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show remote-mirroring

Display the remote mirroring configuration information.

Syntax

show remote-mirroring interfaces <gigabitEthernet> [enable] [mode <source|termination>] [srcMac <0x00:0x00:0x00:0x00:0x00:0x00>] [dstMac <0x00:0x00:0x00:0x00:0x00:0x00>] [ether-type <0x00-0xffff>] [vlan-id <1-4084>]

Parameters

Variable	Value
dstMac <*0x00:0x00:0x00:0x00:0x00:0x00*>	Sets the destination MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent to this MAC address. The DstMac is used only for RMS ports. For RMT ports, one of the unused MAC addresses from the switch port MAC address range is used. This MAC address is saved in the configuration file.
enable	Enables remote mirroring on the port. When remote mirroring is enabled, the following events occur: • A static entry for the DstMac is added to the Forwarding Database (FDB). All packets that come with this remote mirroring DstMac are sent to the RMT port. • The switch periodically (once in 10 seconds) transmits broadcast Layer 2 packets in the associated VLAN so that all nodes in the network can learn the DstMac.
ether-type <*0x00-0xffff*>	Specifies the Ethertype of the remote mirrored packet. The default value is 0x8103.
mode <source|termination>	Specifies whether the port is an RMT (mode is termination) or an RMS (mode is source).
srcMac <*0x00:0x00:0x00:0x00:0x00:0x00*>	Sets the source MAC address for use in the remote mirroring encapsulation header. The mirrored packet is sent from the RMS port, and the source MAC parameter in the header is derived from this address. The source MAC address of the encapsulated frame contains the first 45 bits of this MAC address. The three least significant bits are derived from the port number of the RMS port. The MAC address of the port is used as the default value.
vlan-id <*1-4084*>	Specifies to which VLAN the remote mirroring destination MAC address belongs. This must be a port-based VLAN. Used only for Remote Mirroring Termination (RMT) ports. When the RMT port is removed from the last VLAN in the list, RMT is disabled on the port.

Default

None

Command mode

Global Configuration mode

show snmplog

View the contents of the SNMP log.

Note:

The following command is only applicable to log files generated by past releases prior to Release 3.2. The command is replaced by `show logging file module snmplog` for new files.

Syntax

`show snmplog`

Parameters

Variable	Value
file	Displays SNMP log file.
grep *WORD <1–255>*	Displays a particular string.
tail	Displays the SNMP log file from the tail.

Default

None

Command mode

Privileged EXEC mode

show syslog

View the syslog information to ensure accuracy.

Syntax

`show syslog`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show syslog host

View the syslog host information to ensure accuracy.

Syntax

show syslog host <1-10>

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show trace auto

Shows the current configuration for the automatic trace function.

Syntax

show trace auto

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show trace file

View the trace results.

Syntax

show trace file [tail]

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show trace level

Shows the current trace level for all modules.

Syntax

show trace level

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show trace modid-list

Shows the relationship between level number and module ID to use with the trace tool.

Syntax

show trace modid-list

Parameters

None

Default

None

Command mode

Privileged EXEC mode

snmplog

Use SNMP trap logging to log to the system log file. This allows you to send SNMP logs to a system log server.

Syntax

snmplog enable

snmplog disable

Parameters

None

Default

Disabled.

Command mode

Global Configuration mode

snmp-server host v1

Configure an SNMP host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

snmp-server host WORD <1–256> port <1–65535> v1 WORD<1–32> [filter WORD<1–32>]

Parameters

Variable	Value
WORD<1–256>	Specifies either an IPv4 or IPv6 address.
port*<1–65535>*	Specifies the host server port number.

Variable	Value
v1 *WORD <1–32>* [filter *WORD<1–32>*	Creates a new SNMPv1 entry for the target address table. • *WORD<1–32>* specifies the security name, which identifies the principal that generates SNMP messages. • filter *WORD<1–32>* specifies the filter profile to use.

Default

None

Command mode

Global Configuration mode

snmp-server host v2

Configure an SNMPv2 host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

snmp-server host WORD <1–256> port <1–65535> v2c WORD<1–32> {inform [mms <0–2147483647>] [retries <0–255>] [timeout <0–2147483647>]} [filter WORD<1–32>]

Parameters

Variable	Value
v2c *WORD<1–32>* {inform [mms *<0–2147483647>*[[retries *<0–255>*] [timeout *<0–2147483647>*]} [filter *WORD<1–32>*]	Creates a new SNMPv2c entry for the target address table. • *WORD <1–32>* specifies the security name, which identifies the principal that generates SNMP messages. • inform indicates that SNMP notifications should be sent as inform (rather than trap). • mms*WORD <0–2147483647>* specifies the maximum message size as an integer with a range of 1 to 2147483647. • retries*WORD <0–255>* specifies the retry count value with a range of 0 to 255.

Variable	Value
	• timeout*WORD <0–2147483647>* specifies the timeout value in seconds with a range of 0 to 214748364. • filter*WORD <1–32>* specifies the filter profile to use.

Default

None

Command mode

Global Configuration mode

snmp-server host v3

Configure an SNMPv3 host so that the switch can forward SNMP traps to a host for monitoring.

Syntax

snmp-server host WORD<1–256> port <1–65535> v3 {noAuthnoPriv|authnoPriv|AuthPriv} WORD <1–32> {inform [retries <0–255>] [timeout <1–2147483647>]} [filter WORD<1–32>]

Parameters

Variable	Value
v3 {noAuthnoPriv|authNoPriv|AuthPriv} {inform [retries *WORD<0–255>*] [timeout *<1–2147483647>*]} [filter *WORD<1–32>*	Creates a new SNMPv3 entry for the target address table. • {noAuthnoPriv|authNoPriv|AuthPriv} specifies the security level. • *WORD <1–32>* specifies the security name, which identifies the principal that generates SNMP messages. • inform indicates that SNMP notifications should be sent as inform (rather than trap). • retries*WORD <0–255>* specifies the retry count value with a range of 0 to 255.

Variable	Value
	• timeout*WORD <1–2147483647>* specifies the timeout value in seconds with a range of 1 to 214748364. • filter*WORD <1–32>* specifies the filter profile to use.

Default

None

Command mode

Global Configuration mode

snmp-server notify-filter

Configure the notify table to select management targets to receive notifications, as well as the type of notification to send to each management target.

Syntax

`snmp-server notify-filter WORD<1-32> WORD<1-32>`

Parameters

Variable	Value
WORD<1-32> WORD<1-32>	Creates a notify filter table. • *WORD<1-32>* specifies the name of the filter profile with a string length of 1 to 32. • The second *WORD<1-32>* identifies the filter subtree OID with a string length of 1 to 32. If the Subtree OID parameter uses a '+' prefix (or no prefix), this indicates include. If the Subtree OID uses the '-' prefix, this indicates exclude.

Default

None

Command mode

Global Configuration mode

snmp-server sender-ip

Configure the IP interface from which the SNMP traps originate if the Virtual Services Platform 9000 has multiple interfaces.

Syntax

`snmp-server sender-ip <A.B.C.D> <A.B.C.D>`

Parameters

Variable	Value
`sender-ip <A.B.C.D> <A.B.C.D>`	Configures the SNMP trap receiver and source IP addresses. Specify the IP address of the destination SNMP server that will receive the SNMP trap notification in the first IP address. Specify the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If this is set to 0.0.0.0 then the switch uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
`agent-conformance enable`	Enables the agent conformance mode. Conforms to MIB standards when disabled. If you activate this option, feature configuration is stricter and error handling less informative. Activating this option is not a recommended or normally supported mode of operation.
`authentication-trap enable`	Activates the generation of authentication traps.
`force-iphdr-sender enable`	Enables the automatic configuration of the SNMP and IP sender to the same value. The default is false.

Variable	Value
`force-trap-sender enable`	Enabled sending the configured source address (sender IP) as the sender network in the notification message.

sys force-msg

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After you enable the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Syntax

`sys force-msg WORD<4-4>`

`no sys force-msg WORD<4-4>`

Parameters

Variable	Value
WORD<4-4>	Adds a forced message control pattern. *WORD<4-4>* is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes matching one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table, including a wildcard pattern (****). If you specify the wildcard pattern, all messages undergo message control.

Default

None

Command mode

Global Configuration mode

sys msg-control

Configure system message control to suppress duplicate error messages on the console and to determine the action to take if they occur.

Syntax

sys msg-control [action <both|send-trap|suppress-msg>] [control-interval <1-30>] [max-msg-num <2-500>]

default sys msg-control [action] [control-interval] [max-msg-num]

no sys msg-control

Parameters

Variable	Value
action <both|send-trap| suppress-msg>	Configures the message control action. You can either suppress the message or send a trap notification, or both.
control-interval *<1-30>*	Configures the message control interval in minutes.
max-msg-num *<2-500>*	Configures the number of occurrences of a message after which the control action occurs.

Default

The default is disabled. The following list provides the default values for the applicable command parameters:

- action: suppress-msg
- control-interval: 5 minutes
- max-msg-num: 5 messages

Command mode

Global Configuration mode

syslog enable

The syslog commands control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

Syntax

syslog enable

Parameters

Variable	Value
`enable`	Enables the sending of syslog messages on the switch.

Default

None

Command mode

Global Configuration mode

Related commands

Variable	Value
`ip-header-type <default|circuitless-ip|management-virtual-ip>`	Specifies the IP header in syslog packets to default, circuitless-ipor management-virtual-ip. • If set to default, then for syslog packets that are transmitted in-band via input/output (I/O) ports, the IP address of the VLAN is used. For syslog packets that are transmitted out-of-band through the management port, the physical IP address of the Master CPU is used in the IP header. • If set to management-virtual-ip, then for syslog packets that are transmitted out-of-band only through the management port, the virtual management IP address of the switch is used in the IP header. • If set to circuitless-ip, then for all syslog messages (in-band or out-of-band), the circuitless IP address is used in the IP header. If a user has configured multiple CLIPs, the first CLIP configured is used.
`max-hosts <1-10>`	Specifies the maximum number of syslog hosts supported. **`<maxhost>`** is the maximum number of enabled hosts allowed (1 to 10).

syslog host

The syslog commands control a facility in UNIX machines that logs SNMP messages and assigns each message a severity level based on importance.

Syntax

`syslog host <1-10>`

Parameters

Variable	Value
address*WORD<0–46>*	Configures a host location for the syslog host. **WORD<0-46>** is the IP address of the UNIX system syslog host.
facility {local0|local1|local2|local3|local4|local5|local6|local7}	Specifies the UNIX facility used in messages to the syslog host. **{local0|local1|local2|local3|local4|local5|local6|local7}** is the UNIX system syslog host facility (LOCAL0 to LOCAL7).
host	Specifies host settings.
enable	Enables the syslog host.
maperror {emergency|alert|critical|error|warning|notice|info|debug}	Specifies the syslog severity to use for Error messages.
mapfatal {emergency|alert|critical|error|warning|notice|info|debug}	Specifies the syslog severity to use for Fatal messages.
mapinfo {emergency|alert|critical|error|warning|notice|info|debug}	Specifies the syslog severity level to use for Information messages.
mapwarning {emergency|alert|critical|error|warning|notice|info|debug}	Specifies the syslog severity to use for Warning messages.
severity <info|warning|error|fatal>	Specifies the severity levels for which syslog messages should be sent for the specified modules.
udp-port <514-530>	Specifies the UDP port number on which to send syslog messages to the syslog host. This is the UNIX system syslog host port number (514 to 530).

Default

None

Command mode

Global Configuration mode

trace auto

Use automatic trace to automatically perform the trace function after a parameter reaches a threshold

Syntax

trace auto disable

trace auto enable

trace auto high-percentage <60-100>

trace auto high-track-duration <3-10>

trace auto low-percentage <50-90>

trace auto low-track-duration <3-10>

trace auto module add <0-107> <0-4>

trace auto module remove <0-107>

Parameters

Variable	Value
disable	Disables the automatic trace feature.
enable	Enables automatic trace feature.
high-percentage *<60–100>*	Specifies the high-percentage threshold for a module. The range is 60–100%.
high-track-duration *<34–10>*	Specifies, in seconds, the amount of time that the activity must be sustained to trigger the trace.
low-percentage *<50–90>*	Specifies the low-percentage threshold below which autotrace is disabled.
low-track-duration *<3–10>*	Specifies, in seconds, the amount of time that the activity must be sustained to trigger the trace.
module add *<0-107>* *<0-4>*	Configures the trace auto-enable function by specifying the module ID and level. • *<0–107>* identifies the module that you want to add. • *<0-4>*specifies the trace level from 0–4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose. See show trace modid-list on page 580 to determine module ID for which you want to use the trace tool.
module remove	Removes a module ID from the automatic trace instance.

Default

The default high-percentage is 90%. The default high-track-duration and low-track-duration is 5 seconds. The default low-percentage is 75%.

Command mode

Privileged EXEC mode

trace flags

Enables or disables OSPFv2 trace flags for debugging. The flags you set are used by the **trace level** command.

Syntax

trace flags ospf set <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>

trace flags ospf remove <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>

Parameters

Variable	Value
remove <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>	Removes the OSPF trace flags for the specified option.
set <none|all|tx-hello|rx-hello|tx-ddp-pkt|rx-ddp-pkt|tx-lsu-pkt|rx-lsu-pkt|tx-lsack|rx-lsack|tx-lsr|rx-lsr|pkt-err|nbr-mismatch|flood|spf-intra|spf-inter|spf-extern|spf-tree|nbr-change|intf-change|abr-lsa-generate|asbr-lsa-generate|dr|dd-masterslave|auth-fail|config|lsa|policy>	Sets the OSPF trace flags for the specified option.

Default

By default, all flags are turned off.

Command mode

Privileged EXEC mode

trace grep

Search trace results for a specific string value, for example, the word error.

Syntax

`trace grep WORD<0-128>`

`trace grep`

Parameters

Variable	Value
WORD<0-128>	Specifies the search keyword. You can use a specific MAC address or search for errors, using the command, `trace grep error`.

Default

None

Command mode

Privileged EXEC mode

trace ipv6 base

Configures trace parameters for the IPv6 base.

Syntax

`trace ipv6 base disable <all|debug|error|icmp|info|ipclient|nbr|pkt|warn>`

`trace ipv6 base enable <all|debug|error|icmp|info|ipclient|nbr|pkt|warn>`

Parameters

Variable	Value
<all|debug|error|icmp|info|ipclient|nbr|pkt|warn>	Specifies the trace category.

Variable	Value
disable	Disables the trace.
enable	Enables the trace.

Default

None

Command mode

Privileged EXEC mode

trace ipv6 forwarding

Configures trace parameters for IPv6 forwarding.

Syntax

trace ipv6 forwarding disable <all|debug|error|info|pkt|warn>

trace ipv6 forwarding enable <all|debug|error|info|pkt|warn>

Parameters

Variable	Value
<all|debug|error|info|pkt|warn>	Specifies the trace category.
disable	Disables the trace.
enable	Enables the trace.

Default

None

Command mode

Privileged EXEC mode

trace ipv6 nd

Configures trace parameters for IPv6 neighbor discovery.

Syntax

trace ipv6 nd disable <all|debug|error|info|nbr|pkt|redirect|warn>

trace ipv6 nd enable <all|debug|error|info|nbr|pkt|redirect|warn>

Parameters

Variable	Value
<all|debug|error|info|nbr|pkt|redirect|warn>	Specifies the trace category.
disable	Disables the trace.
enable	Enables the trace.

Default

None

Command mode

Privileged EXEC mode

trace ipv6 rtm

Configures trace parameters for the IPv6 routing table manager.

Syntax

trace ipv6 rtm disable <all|change-list|debug|error|fib|info|redist|update|warn>

trace ipv6 rtm enable <all|change-list|debug|error|fib|info|redist|update|warn>

Parameters

Variable	Value
<all|change-list|debug|error|fib|info|redist|update|warn>	Specifies the trace category.
disable	Disables the trace.
enable	Enables the trace.

Default

None

Command mode

Privileged EXEC mode

trace ipv6 transport

Configures trace parameters for IPv6 transport.

Syntax

`trace ipv6 transport disable <all|common|tcp|udp>`

`trace ipv6 transport enable <all|common|tcp|udp>`

Parameters

Variable	Value
<all|common|tcp|udp>	Specifies the trace category.
disable	Disables the trace.
enable	Enables the trace.

Default

None

Command mode

Privileged EXEC mode

trace level

Use trace to observe the status of a software module at a given time.

Syntax

`trace level [<0-175>] [<0-4>]`

Parameters

Variable	Value
`level [<0-175>] [<0-4>]`	Starts the trace by specifying the module ID and level. • **`<0-175>`** specifies the module ID. • **`<0-4>`** specifies the trace level from 0 to 4, where 0 is disabled; 1 is very terse; 2 is terse; 3 is very verbose, 4 is verbose.

Default

None

Command mode

Privileged EXEC mode

trace screen

Configures if the system displays trace information on screen.

Syntax

trace screen disable

trace screen enable

Parameters

Variable	Value
disable	Prevents the trace messages from appearing on screen.
enable	Shows the trace messages on screen.

Default

None

Command mode

Privileged EXEC mode

traceroute

Use traceroute to determine the route packets take through a network to a destination.

Syntax

traceroute <A.B.C.D> [<1-1464>] [-m <1-255>] [-p <0-65535>] [-q <1-255>] [-w <1-255>] [-v] [source WORD <1-256>] [vrf WORD <0-16>]

Parameters

Variable	Value
-m <1-255>	Specifies the is maximum time-to-live (TTL) (1 to 255).

Variable	Value
`-p <0-65535`	Specifies the base UDP port number (0 to 65535).
`-q <1-255>`	Specifies the number of probes per TTL (1 to 255).
`-v`	Specifies verbose mode (detailed output).
`-w <1-255>`	Specifies the wait time per probe (1 to 255).
`<1-1464>`	Specifies the size of the probe packet (1 to 1464).
`source WORD<1-256>`	Specifies the source IP address for use in traceroutes.
`vrf WORD<0-16>`	Specifies the VRF instance by VRF name.

Default

None

Command mode

Privileged EXEC mode

Chapter 17: Upgrade commands

This chapter provides the Avaya Command Line Interface (ACLI) commands to upgrade the Avaya Virtual Services Platform 9000.

backup

Use this command to backup all files, including the directory, of the internal flash or external flash to the USB flash.

Important:

You must disable logging to the compact flash you want to restore before you can use the **backup** command.

The system verifies that the USB flash device has enough available space to perform the backup operation. If the USB flash device does not have enough available space, an error message appears. The backup command uses the following filepath on the USB flash device: `/usb/intflash/intflashbackup_yyyymmddhhmmss.tgz` and `/usb/extflash/extflashbackup_yyyymmddhhmmss.tgz`.

Syntax

`backup <intflash|extflash>`

Parameters

Variable	Value
intflash	Specifies the internal flash to back up.
extflash	Specifies the external flash to back up.

Default

None

Command mode

Privileged EXEC mode

copy

Copy files as part of an upgrade procedure to back up files or to move files to another location.

Syntax

copy WORD<1–255> WORD<1–255> [-y]

copy clilog WORD<1–255>

copy running-config startup-config

Parameters

Variable	Value
clilog *WORD<1–255>*	Copies the log file to a specific location. You can specify the name and location for the log file in one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /extflash/<file> • /mnt/intflash/<file> • /mnt/extflash/<file> • /usb/<file>
running-config startup-config	Copies the running configuration file to /intflash/config.cfg by default.
WORD<1–255> *WORD<1–255>*	Specifies the name and location of the file to copy. You can specify the name and location in one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /extflash/<file> • /mnt/intflash/<file> • /mnt/extflash/<file> • /usb/<file> The first*WORD<1–255>* identifies the source location and file name. The second *WORD<1–255>* identifies the destination location and file name.

Variable	Value
-y	Suppresses the confirmation message before the file copies. If you omit this parameter, you are asked to confirm the action before the switch copies the file.

Default

None

Command mode

Privileged EXEC mode

dir

View the free space and files in flash memory.

Syntax

`dir -l`

`dir -r`

`dir WORD<1-99>`

`dir`

Parameters

Variable	Value
-l	Displays all the details of all the files like name, size and time and date of the file created.
-r	Displays the recursive directories.
Word <1-99>	Specifies the name of the particular file to view details.

Default

None

Command mode

Privileged EXEC mode

dos-chkdsk

Checks MS DOS file system for any inconsistencies.

Syntax

dos-chkdsk WORD <1–99> repair

Parameters

Variable	Value
WORD <1–99>	Specifies the device name to repair which is /extflash or /usb.
repair	Repairs the errors found.

Defaults

None

Command mode

Privileged EXEC mode

dos-format

Formats the external flash or USB.

Syntax

dos-format WORD <1–99>

Parameters

Variable	Value
WORD <1–99>	Specifies the device name to format which is /extflash or /usb.

Defaults

None

Command mode

Privileged EXEC mode

remove

Remove files to make space.

Syntax

`remove WORD<1-255> <file>[-y]`

Parameters

Variable	Value
WORD<1-255>	*WORD<1-255>* specifies the file to remove.
WORD<1-255><file>	Specifies the file name to remove in one of the following formats: • /intflash/ <file> • /extflash/ <file> • /usb/<file> • /mnt/intflash/ <file> • /mnt/extflash/ <file> /mnt/intflash is the internal flash of the second CP module (the one to which you are not connected) /mnt/extflash is the external flash of the second CP module (the one to which you are not connected) *WORD<1–255>* is a string of 1–255 characters.
`-y`	Skip the confirm question.

Default

None

Command mode

Privileged EXEC mode

show boot config choice

Make copies of the configuration files before you upgrade the switch software.

Syntax

`show boot config choice`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show boot config flags

Verify your upgrade by viewing bootconfig flags to ensure proper switch operation.

Syntax

`shoe boot config flags`

Parameters

None

Defaults

None

Command mode

Privileged EXEC mode

show software

Display unpacked software releases information.

Syntax

`show software [detail] [WORD <1–99>]`

Parameters

Variable	Value
detail	Displays software release in detail mode.
<*WORD 1-99*>	Specifies a specific software release to be displayed in the range of 1 to 99.

Default

None

Command mode

Privileged EXEC mode

show software patch

Displays the unpacked software patching information that is to be updated on the chassis of the switch.

Syntax

`show software patch`

Parameters

Variable	Value
all	Displays the patch status for all the valid patches.
applied	Displays patches that are currently applied and active.
candidate	Displays patches that are eligible for activation against the active software version.
detail	Displays detailed patch status information.
patch-ids *WORD <1–255>*	Displays information for the specified patch ids. *WORD <1–255>* specifies the name of the patch file for the information to be displayed.
verbose	Displays verbose patch status information.
version *WORD <1–255>*	Specifies the software version used to display the software patches that are candidate or applied.

Default

None

Command mode

Privileged EXEC mode

show sys software

Verify that the image and configuration are loaded properly.

Syntax

show sys software

Parameters

None

Defaults

None

Command mode

Privileged EXEC mode

slot reset

Use the following command after all modules are updated, for the updates to take effect on the switch.

Syntax

slot reset <1–12>

slot reset SF1

slot reset SF2

slot reset SF3

slot reset SF4

slot reset SF5

slot reset SF6

Parameters

Variable	Value
<1–12>	Specifies the slot number. Valid slots are 1 to 12.
SF1	Specifies Switch Fabric 1.
SF2	Specifies Switch Fabric 2.

Variable	Value
SF3	Specifies Switch Fabric 3.
SF4	Specifies Switch Fabric 4.
SF5	Specifies Switch Fabric 5.
SF6	Specifies Switch Fabric 6.

Default

None

Command mode

Privileged EXEC mode

software

Perform various software functions on the switch to ensure it is updated with latest versions.

Syntax

`software [activate WORD<1–99>|add WORD<1–99>|add-modules WORD<1–99>|commit|remove WORD<1–99>]`

Parameters

Variable	Value
activate	Copies the software version to the boot flash file. When you use the **`software activate`** command, the system checks for hardware dependencies and prevents a downgrade if it detects a dependency. For example, if a hardware component has a minimum software version dependency, you cannot downgrade to an incompatible software version or install the hardware component in a chassis that runs an incompatible software version.
add	Unpacks a software release <version>.
add-modules	Adds modules to existing software release in /intflash|release|<version>.
commit	Ensures the running software release is trusted.
remove	Removes the software release <version>.

Default

None

Command mode

Privileged EXEC mode

software patch

Performs various software patch functions to keep the switch updated with the latest releases and software versions and utilize the switch optimally.

Syntax

software patch abort

software patch add WORD <1–255>

software patch apply [all] [all version WORD<1–255>][hitless][reset] [commit][revert all][revert hitless][revert reset][remove WORD<1–00>]

software patch apply patch-ids WORD<1–255> [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>]

software patch remove version WORD<1–255> patch-id WORD<1–255>

software patch revert patch-ids WORD<1–255> [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>] [WORD<1–255>]

Parameters

Variable	Value
abort	Cancels the software patch apply/revert.
add *WORD <1–255>*	Unpacks the software patches to /intflash|release|<version>|patches|<patch-id> where <version> and <patch-id> are extracted from the patch file. *WORD <1–255>* specifies the patch file name in the range of 1 to 255.
apply [all|hitless|patch-ids <WORD<1–255>|reset] version *WORD<1–255>*	Applies the latest versions of patches available to the switch. Apply the following: • all — all software patches • hitless — hitless software patches

Variable	Value
	• patch-ids — software patch ID • reset — reset software patches *WORD<1–255>* specifies the name of the software version that needs to be applied on the switch.
commit	Commit the patch to apply or revert process on the switch.
remove version *WORD<1–255>* patch-id *WORD<1–255>*	Removes patches from /intflash|release|<version>|patches|<patch-id>. *WORD<1–255>* specifies the name of the software version. *WORD<1–255>* specifies the name of the patch file.
revert [all|hitless|patch-ids <WORD <1–255>|reset] version *WORD <1–255>*	Resets or unapplies all the versions of the patches applied on the switch. Revert the following: • all — all software patches • hitless — hitless software patches • patch-ids — software patch ID • reset — reset software patches *WORD <1–255>* specifies the name of the software version that needs to be reverted on the switch.

Default

None

Command mode

Privileged EXEC mode

sys action cpu-switch-over

Perform the switch over of the CPU while hot-swapping the master CP module in a dual CP module chassis.

Syntax

`sys action cpu-switch-over`

Parameters

Variable	Value
cpu-switch-over	Switches over to the other CPU.

Defaults

None

Command mode

Global Configuration mode

Related Parameters

Variable	Value
reset	Resets console or counters in a CPU.

sys software auto-commit

Enables the auto-commit feature for software upgrades. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you do not enable the auto-commit option, you must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (commited) version.

Syntax

`sys software auto-commit enable`

`default sys software auto-commit enable`

`no sys software auto-commit enable`

Parameters

None.

Default

The default is enabled.

Command mode

Global Configuration mode

sys software commit-time

Configures the commit feature for software upgrades to allows maximum time to ensure that the upgrade is successful. You must enter the software commit command before the commit timer expires to commit the new software version otherwise the system restarts automatically to the previous (commited) version.

Syntax

sys software commit-time <10–60>

default sys software commit-time

Parameters

Variable	Value
<10–60>	Specifies the commit timer in minutes.

Default

The default is 10 minutes.

Command mode

Global Configuration mode

sys software patch

Configures the software patch.

Syntax

sys software patch file-path WORD<1–255>

default sys software patch file-path

Parameters

Variable	Value
WORD<1–255>	Specifies the location of the file to patch.

Default

None.

Command mode

Global Configuration mode

Chapter 18: VLAN and spanning tree commands

This chapter describes the Avaya command line interface (ACLI) commands to help you to configure and manage virtual local area networks (VLAN) and Spanning Tree on the Avaya Virtual Services Platform 9000.

auto-recover-port port enable

Enable or disable autorecovery on a port.

Syntax

auto-recover-port [port {slot/port [-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	Enables spoof detection on the port.
port *{slot/port [-slot/port][,...]}*	Specifies the port list.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

brouter

Configure a port as a brouter port.

Syntax

brouter port {slot/port} [vlan <2–4084>] [subnet <{A.B.C.D/X}|{A.B.C.D}>] [mac-offset <0–65535>]

brouter vlan <2–4084> [subnet <{A.B.C.D/X}|{A.B.C.D} {A.B.C.D}>] [mac-offset <0–65535>]

no brouter [port {slot/port}]

Parameters

Variable	Value
vlan *<2–4084>*	Specifies the VLAN ID.
mac-offset *<0–65535>*	Specifies the Mac-offset value.
subnet *<{A.B.C.D/X}|{A.B.C.D}>*	Assigns an IP address and mask for the management port.
port *{slot/port}*	Specifies the slot and port.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

default-vlan-id

Configure the default VLAN ID for the port.

Syntax

default-vlan-id [port {slot/port[-slot/port][,...]}] <0–4084>

Parameters

Variable	Value
<0–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Interface Configuration mode

dsapssap

Configure the multiple DSAP and SSAP to create a protocol-based VLAN.

Syntax

dsapssap <0x0-0xffff>

Parameters

None

Default

None

Command mode

VLAN Interface Configuration mode

encapsulation dot1q

Enable tagging on the ports before configuring Untagged VLANs.

Syntax

encapsulation dot1q port {slot/port [-slot/port][,...]}

Parameters

None

Default

None

Command mode

GigabitEthernet Inteface Configuration mode

ip address (on a VLAN)

Assign an IP address to a VLAN to configure the VLAN.

Syntax

ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> [<0-1535>]

Parameters

Variable	Value
<A.B.C.D/X>|<A.B.C.D> <A.B.C.D>	Specifies the IP address and subnet mask in the format A.B.C.D/X or A.B.C.D A.B.C.D.
<0–1535>	Specifies the Mac-offset value. The value is in the range of 0–1535.

Default

None

Command mode

VLAN Interface Configuration mode

ip arp multicast-mac-flooding

Determines whether ARP entries for multicast MAC addresses are associated with the VLAN or the port interface on which they were learned. Links the ARP entry for the Network Load Balancer (NLB) cluster to the multicast group ID (MGID) of the VLAN.

Syntax

`ip arp multicast-mac-flooding`

`default ip arp multicast-mac-flooding`

`no ip arp multicast-mac-flooding`

Parameters

None

Default

The default is disabled.

Configuration mode

Global Configuration mode

loop-detect arp-detect

Configure the Loop Detection to detect the MAC addresses that are looping from one port to another port.

Syntax

`loop-detect arp-detect`

Parameters

Variable	Value
action	Specifies the loop detect action to be taken.
arp-detect	The Address Resolution Protocol (ARP)-Detect feature is used for IP configured interfaces for ARP packets. Enable this feature (in addition to loop detection) on routed interfaces.

Default

None

Command mode

Global Configuration mode

mac-security add

Enable global MAC security to filter out (drop) packets that contains certain MAC addresses as source or destination. Configure a set of MAC addresses.

Syntax

`mac-security add 0x00:0x00:0x00:0x00:0x00:0x00`

Parameters

Variable	Value
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the MAC address.

Default

None

Command mode

Global Configuration mode

mac-security limit-learning

Limit MAC address learning to limit the number of forwarding database entries to protect the FDB.

Syntax

mac-security limit-learning [port {slot/port[-slot/port] [,...]}] enable [max-addrs <1–64000>] [min-addrs <0–64000>] [snmp-trap] [violation-down-port]

Parameters

Variable	Value
enable	Limits the MAC learning for the port. This feature does not affect the forwarding of the packets. If you enable limit-learning, the FDB entry for each port is limited to the number you specify in max-addrs. If you enable the auto-learn parameter, after the maximum addresses are learned, all the new SA MAC packets are dropped. This feature provides no value if you enable unknown-mac-discard and disable auto-learn because all unknown packets are dropped. Do not enable auto-learning and limit-learning simultaneously
max-addrs *<1–64000>*	Specifies the maximum number of MAC address to learn. After the maximum value is reached, no further MAC learning occurs. The system does not drop packets; it forwards packets.
min-addrs *<0-64000>*	Specifies the minimum number of MAC addresses to learn. MAC learning restarts after the FDB entry count reaches the value you specify in min-addrs.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
snmp-trap	Enables logging and SNMP traps for violations.
violation-down-port	Disables the port on violation.

Default

The following list provides command defaults:

- max-addrs: 1024
- min-addrs: 512
- snmp-trap: disabled
- violation-down-port: disabled

Command mode

GigabitEthernet Interface Configuration mode

mac-security unknown-discard

Discard all the unknown MACs to limit the number of forwarding database entries learned on a port to a user-specified value.

Syntax

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] enable

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 [auto]

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] violation-down-port

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] violation-logging

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] violation-send_authentication-trap

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] auto-learning enable

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] auto-learning learning-mode <one-shot|continuous>

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] auto-learning lock-learning-mac

mac-security unknown-discard [port {slot/port[-slot/port] [,...]}] auto-learning max-addrs <0–2048>

Parameters

Variable	Value
allow-mac *0x00:0x00:0x00:0x00:0x00:0x00* [auto]	Add allowed MAC address of the port. *0x00:0x00:0x00:0x00:0x00:0x00* specifies the auto-learned MAC address.
enable	Enables unknown MAC discard of the port.
learning-mode <one-shot|continuous>	Specifies the learning mode as one of the following: • one-shot: The autolearned addresses do not age out. When the VLAN mac-addressentry is flushed, the autolearned addresses are not flushed. • continuous: In continuous mode the aging of the autolearned MAC is subject to the normal aging. When the VLAN macaddress- entry is flushed, the autolearned addresses are also flushed.
lock-learning-mac	Saves autolearned addresses when you save the configuration file.
max-addrs *<0–2048>*	Specifies the total number of unknown MAC addresses to learn.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
violation-down-port	Configures the violation down port action of the port.
violation-logging	Configures the violation logging action of the port.
violation-send-authentication-trap	Configures the violation send authentication trap action of the port.

Default

The following list provides command defaults:

- enable: disabled
- max-addrs : 2048
- violation-down-port: disabled
- violation-logging: enabled
- violation-send-authentication-trap: disabled
-

Command mode

GigabitEthernet Interface Configuration mode

nlb-mode

Configure the NLB support on an IP interface to enable or disable the Network Load Balancer (NLB) support.

Syntax

nlb-mode <igmp-mcast|multicast|unicast>

Parameters

None

Default

None

Command mode

VLAN Interface Configuration mode

policy-vlan-precedence port

Use this command to indicate whether source MAC or IP subnet VLAN classification takes precedence.

Syntax

policy-vlan-precedence [port {slot/port [-slot/port][,...]}] {source-mac|subnet}

Parameters

Variable	Value
port *{slot/port [-slot/port][,...]}*	Specifies the slot and the port number.
{source-mac|subnet}	Indicates that the source MAC-based or subnet-based VLAN classification takes precedence.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

protocol-vlan

Enable protocol-based VLAN on the port.

Syntax

protocol-vlan [port {slot/port[-slot/port][,...]}] enable

default protocol-vlan [port {slot/port[-slot/port][,...]}] enable

no protocol-vlan [port {slot/port[-slot/port][,...]}] enable

Parameters

Variable	Value
enable	Enables or disables protocol-based VLAN for the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is enabled.

Command mode

GigabitEthernet Interface Configuration mode

show interfaces vlan

Show basic and advanced VLAN information.

Syntax

show interfaces vlan [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan arp

Display Address Resolution Protocol (ARP) information for the VLAN.

Syntax

show interfaces vlan arp [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan autolearn-mac

Show bridging autolearn MAC address information for VLANs.

Syntax

show interfaces vlan autolearn-mac

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan dhcp-relay

Show DHCP information for the VLAN.

Syntax

show interfaces vlan dhcp-relay [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan igmp

Shows Internet Group Management Protocol (IGMP) information for the VLAN.

Syntax

show interfaces vlan igmp [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan igmp-mrdisc

Show IGMP multicast route discovery information for the VLAN.

Syntax

show interfaces vlan igmp-mrdisc [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan ip

Show the IP configuration for the VLAN.

Syntax

show interfaces vlan ip [<1–4084>] [vrf WORD<0–16>] [vrfids WORD<0–512>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
vrf *WORD<0–16>*	Specifies a VRF by name.
vrfids *WORD<0–512>*	Specifies a range of VRF IDs.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan manual-edit-mac

Displays the manually-edited bridging MAC address information for VLANs.

Syntax

show interfaces vlan manual-edit-mac

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan nlb-mode

Shows the Network Load Balancer (NLB) configuration for the VLAN.

Syntax

show interfaces vlan nlb-mode [<1–4084>]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan vlan-bysrcmac

Shows source MAC-based VLAN information.

Syntax

`show interfaces vlan vlan-bysrcmac`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show interfaces vlan vrfs

Shows VRF-association information for the VLAN.

Syntax

`show interfaces vlan vrfs [<1–4084>] [vrf WORD<0–16>] [vrfids WORD<0–512>] [{slot/port [-slot/port][,...]}]`

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
vrf *WORD<0–16>*	Specifies a VRF instance by name.
vrfids *WORD<0–512>*	Specifies a range of VRFs by ID number.

Default

None

Command mode

Privileged EXEC mode

show interface vlan nlb-mode

Use the following command to view Network Load Balancing-mode (NLB-mode) information.

Syntax

`show interface vlan nlb-mode <1–4084>`

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID in a range of 1–4084.

Default

None

Command mode

VLAN Interface Configuration mode

show mac-address-entry

Shows the database status and MAC address to display the static forwarding database status.

Syntax

`show mac-address-entry`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree config

Query the change detection setting to show the port information.

Syntax

`show spanning-tree config`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp config

View the MSTP configurations to display the MSTP-related bridge-level VLAN and region information.

Syntax

show spanning-tree mstp config

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp msti config

Displays the configuration for one or all Multiple Spanning Tree Protocol (MSTP) instance IDs.

Syntax

show spanning-tree mstp msti config [<1–63>]

Parameters

Variable	Value
<1–63>	Specifies the MSTP instance ID.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp msti port

Shows the configuration, role, or statistics information of an MSTP port.

Syntax

show spanning-tree mstp msti port config [{slot/port [-slot/port] [,...]}]

show spanning-tree mstp msti port role [{slot/port [-slot/port] [,...]}]

show spanning-tree mstp msti port statistics [{slot/port [-slot/port] [,...]}]

Parameters

Variable	Value
config *{slot/port [-slot/port][,...]}*	Shows the configuration information of an MSTP port.
role *{slot/port [-slot/port][,...]}*	Shows the role information of an MSTP port.
statistics *{slot/port [-slot/port][,...]}*	Shows the statistics information of an MSTP port.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp port role

Displays Multiple Spanning Tree Protocol (MSTP) port information.

Syntax

show spanning-tree mstp port role [{slot/port[-slot/port][,...]}]

show spanning-tree mstp port config [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
config [{slot/port[-slot/port][,...]}]	Displays the MSTP port configurations, which display MSTP-related bridge-level VLAN and region information.
role [{slot/port[-slot/port][,...]}]	Displays the MSTP port information to display the MSTP, CIST port, and MSTI port information maintained by every port of the common spanning tree.
{slot/port[-slot/port][,...]}	Displays the MSTP port information.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree mstp status

View the MSTP status to display the MSTP- related status information known by the selected bridge.

Syntax

`show spanning-tree mstp status`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp config

View the global RSTP configuration information to display the Rapid Spanning Tree Protocol (RSTP) configuration details.

Syntax

show spanning-tree rstp config

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp port config

Configure Ethernet RSTP parameters to set RSTP parameters for the port.

Syntax

show spanning-tree rstp port config [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Shows RSTP port configuration.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp port role

View the RSTP role to display the RSTP information.

Syntax

show spanning-tree rstp port role [{slot/port[-slot/port][,...]}]

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Shows the RSTP port role.

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp port status

View the RSTP status for a port to display the RSTP related status information for a selected port.

Syntax

`show spanning-tree rstp port status [{slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Privileged EXEC mode

show spanning-tree rstp status

View the RSTP status to display the RSTP related status information for the selected bridge.

Syntax

`show spanning-tree rstp status`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show vlan advance

View the advanced parameters to display the advanced parameters for the specified VLAN or for all VLANs.

Syntax

show vlan advance [<1-4084>]

Parameters

Variable	Value
port <value>	Specifies the port or range of ports.
<1-4084>	Specifies the VLAN ID in a range of 1 to 4084.

Default

None

Command mode

Privileged EXEC mode

show vlan autolearn-mac

View autolearned MAC addresses.

Syntax

show vlan autolearn-mac

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show vlan basic

View the VLAN information to display the basic configuration for all VLANs or a specified VLAN.

Syntax

show vlan basic <1-4084>

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID in a range of 1 to 4084.

Default

None

Command mode

Privileged EXEC mode

show vlan brouter-port

View the brouter port information to display the brouter port VLAN information for all VLANs on the switch or for the specified VLAN.

Syntax

show vlan brouter-port

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show vlan mac-address-entry

View FDB filters to display the FDB filters for the specified VLAN.

Syntax

show vlan mac-address-entry [<1-4084>]

show vlan mac-address-entry mac 0x00:0x00:0x00:0x00:0x00:0x00

show vlan mac-address-entry port {slot/port[-slot/port][,...]}

Parameters

Variable	Value
mac *0x00:0x00:0x00:0x00:0x00:0x00*	Specifies the MAC address.
port {slot/port[-slot/port] [,...]}	Specifies the port or range of ports in either slot or port format.
<1-4084>	Specifies the VLAN ID in a range of 1 to 4084.

Default

None

Command mode

Privileged EXEC mode

show vlan mac-address-static

View the database status, MAC address, and QoS levels to display the static forwarding database status.

Syntax

show vlan mac-address-static [<1-4084>]

Parameters

Variable	Value
mac <*value*>	Specifies the MAC address.
port <*portList*>	Specifies the port or range of ports in either slot or port format.
<*1-4084*>	Specifies the VLAN ID in a range of 1 to 4084.

Default

None

Command mode

Privileged EXEC mode

show vlan manual-edit-mac

Shows the list of manually edited MAC addresses and the associated ports.

Syntax

`show vlan manual-edit-mac`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

show vlan members

View the VLAN port member status to display the port member status for all VLANs on the switch or for the specified VLAN.

Syntax

`show vlan members [<1–4084>][null-vlan] [port {slot/port[-slot/port][,...]}]`

Parameters

Variable	Value
null-vlan	Display ports in a null VLAN. The Virtual Services Platform 9000 supports a placeholder for ports that is called a null port-based VLAN or unassigned VLAN.
<1-4084>	Specifies the VLAN ID in the range of 1 to 4084. **Important:** Entering a VLAN ID is optional. When you enter a VLAN ID, the command shows information for the specified VLAN or port. Without the VLAN ID the command shows information for all the configured VLANs.
port *{slot/port[-slot/port] [,...]}*	Specifies the port or range of ports. **Important:** Entering a port {slot/port[-slot/ port][,...]} is optional. If you enter a port {slot/port[-slot/ port] [,...]}, the command shows information for the port. Without the port {slot/ port[-slot/port][,...]}, the command shows information for all the ports.

Default

None

Command mode

Privileged EXEC mode

show vlan src-mac

View the VLAN source MAC addresses to display the source MAC address for any source MAC-based VLANs on the switch or for the specified VLAN.

Syntax

`show vlan src-mac <1-4084>`

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID. The value ranges from 1 to 4084.

Variable	Value
	Important: The entry of a VLAN ID is optional. When you enter a VLAN ID, the command shows information for the specified VLAN or port. Without the VLAN ID the command shows information for all the configured VLANs.

Default

None

Command mode

Privileged EXEC mode

source-mac-vlan

Enable source MAC-based VLAN on the port.

Syntax

source-mac-vlan [port {slot/port[-slot/port][,...]}] [enable]

default source-mac-vlan [port {slot/port[-slot/port][,...]}] [enable]

no source-mac-vlan [port {slot/port[-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	Enables or disables source MAC-based VLAN for the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is enabled.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp cost

Configure the contribution of this port to the path cost value for the link.

Syntax

`spanning-tree mstp cost <1–200000000>`

`default spanning-tree mstp cost`

Parameters

Variable	Value
<1–200000000>	Specifies the cost value.

Default

The default is 2000000.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp edge-port

Configure the port as an edge port.

Syntax

`spanning-tree mstp edge-port <false|true>`

`default spanning-tree mstp edge-port`

Parameters

Variable	Value
<false|true>	Enables or disables the port as an edge port.

Default

The default is disabled (false).

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp force-port-state

Enable the force-port-state flag.

Syntax

spanning-tree mstp force-port-state enable

default spanning-tree mstp force-port-state

no spanning-tree mstp force-port-state

Parameters

None

Default

The default is enabled.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp forward-time

Configures the MSTP forward delay for the bridge.

Syntax

spanning-tree mstp forward-time <400–3000>

default spanning-tree mstp forward-time

Parameters

Variable	Value
<400–3000>	Configures the MSTP forward delay for the bridge, in hundredths of a second.

Default

None

Command mode

Global Configuration mode

spanning-tree mstp hello-time (on a port)

Configure the hello-time delay for the port.

Syntax

`spanning-tree mstp hello-time <100–1000>`

`default spanning-tree mstp hello-time`

Parameters

Variable	Value
<100–1000>	Configures the hello-time for a port in one hundredths of a second.

Default

The default is 2.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp max-age

Assigns the MSTP maximum age time for the bridge

Syntax

`spanning-tree mstp max-age <600–4000>`

Parameters

Variable	Value
<600–4000>	Assigns the MSTP maximum age time for the bridge, in one hundredths of a second.

Default

None

Command mode

Global Configuration mode

spanning-tree mstp max-hop

Assign the maximum hop count for the bridge..

Syntax

`spanning-tree mstp max-hop <100–4000>`

Parameters

Variable	Value
<100–4000>	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second.

Default

The default is 2000.

Command mode

Global Configuration mode

spanning-tree mstp msti (globally)

Configure Multiple Spanning Tree Protocol to set the MSTP configuration version.

Syntax

`spanning-tree mstp msti <1-63> priority <0-65535>`

`default spanning-tree mstp msti <1-63> priority`

Parameters

Variable	Value
<1-63>	Specifies the instance parameter.
priority <0-65535>	Configures the MSTP bridge priority. Allowed values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

Default

None

Command mode

Global Configuration mode

spanning-tree mstp msti (on a port)

Configure Multiple Spanning Tree Protocol to set the MSTP configuration version.

Syntax

spanning-tree mstp msti <1-63> cost <1–200000000> [force-port-state enable] [priority <0-65535>]

default spanning-tree mstp msti <1-63> cost [force-port-state enable] [priority]

no spanning-tree mstp msti <1-63> port {slot/port[-slot/port][,...]} [force-port-state enable]

Parameters

Variable	Value
<1-63>	Specifies the instance parameter.
cost <1–200000000>	Configures the path cost for the port
force-port-state enable	Enables MSTI learning for the port.
priority <0-65535>	Configures the MSTP bridge priority. Allowed values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp p2p

Specifies the point-to-point status of the LAN segment attached to this port.

Syntax

spanning-tree mstp p2p <auto|force-false|false-true>

default spanning-tree mstp p2p

Parameters

Variable	Value
<auto|force-false|false-true>	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.

Default

The default is auto.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp pathcost-type

Assigns the MSTP default pathcost version.

Syntax

spanning-tree mstp pathcost-type <bits16|bits32>

default spanning-tree mstp pathcost-type

Parameters

Variable	Value
<*bits16*|*bits32*>	Specifies the pathcost value.

Default

The default is 32 bits.

Command mode

Global Configuration mode

spanning-tree mstp port

Configure all MSTP parameters for a port.

Syntax

spanning-tree mstp port {slot/port} cost <1–200000000>

spanning-tree mstp port {slot/port} edge-port <false|true>

spanning-tree mstp port {slot/port} force-port-state enable

spanning-tree mstp port {slot/port} hello-time <100–1000>

spanning-tree mstp port {slot/port} p2p <auto|force-false|false-true>

spanning-tree mstp port {slot/port} priority <0–240>

spanning-tree mstp port {slot/port} protocol-migration <false|true>

default spanning-tree mstp port {slot/port} cost

default spanning-tree mstp port {slot/port} edge-port

default spanning-tree mstp port {slot/port} force-port-state

default spanning-tree mstp port {slot/port} hello-time

default spanning-tree mstp port {slot/port} p2p

default spanning-tree mstp port {slot/port} priority

default spanning-tree mstp port {slot/port} protocol-migration

no spanning-tree mstp port {slot/port} [force-port-state]

Parameters

Variable	Value
<0–240>	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.
<100–1000>	Configures the hello-time for a port in one hundredths of a second.
<1–200000000>	Specifies the cost value.
<auto|force-false|false-true>	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this

Variable	Value
	port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.
edge-port <false|true>	Enables or disables the port as an edge port.
port {slot/port}	Specifies the slot and port to configure.
protocol-migration <false|true>	Configures the protocol migration state of this port.

Default

The following list provides the command defaults:

- cost: 2000000
- edge-port: disabled (false)
- force-port-state: enabled
- hello-time: 2
- p2p: auto
- priority: 128
- protocol-migration: false

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp priority (globally)

Assigns the MSTP bridge priority.

Syntax

spanning-tree mstp priority <0–61440>

default spanning-tree mstp priority

Parameters

Variable	Value
<0–61440>	Assigns the MSTP bridge priority. The values configured for port priority must be in steps of 4096.

Default

The default is 32768.

Command mode

Global Configuration mode

spanning-tree mstp priority (on a port)

Specifies the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

Syntax

`spanning-tree mstp priority <0–240>`

`default spanning-tree mstp priority`

Parameters

Variable	Value
<0–240>	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.

Default

The default is 128.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp protocol-migration

Enables or disables protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

Syntax

spanning-tree mstp protocol-migration <false|true>

default spanning-tree mstp protocol-migration

Parameters

Variable	Value
<false|true>	Configures the protocol migration state of this port.

Default

The default is false.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree mstp region

Assigns the MSTP region.

Syntax

spanning-tree mstp region config-id-sel <0–255> [region-name WORD<1–32>] [region-version <0–65535>]

Parameters

Variable	Value
config-id-sel <0–255>	Assigns the MSTP region configuration ID number.
region-name WORD<1–32>	Assigns the MSTP region name.
region-version <0–65535>	Assigns the MSTP region version.

Default

The default region and version is 0.

Command mode

Global Configuration mode

spanning-tree mstp tx-holdcount

Assigns the MSTP transmit hold count.

Syntax

`spanning-tree mstp tx-holdcount <1–10>`

`default spanning-tree mstp tx-holdcount`

Parameters

Variable	Value
<1–10>	Assigns the MSTP transmit hold count.

Default

The default is 3.

Command mode

Global Configuration mode

spanning-tree mstp version

Configure the MSTP to set the MSTP configuration.

Syntax

`spanning-tree mstp version mstp`

Parameters

None

Default

None

Command mode

Global Configuration mode

spanning-tree rstp cost

Configure the contribution of this port to the path cost value for the link.

Syntax

spanning-tree rstp cost <1–200000000>

default spanning-tree rstp cost

Parameters

Variable	Value
<1–200000000>	Specifies the cost value.

Default

The default is 2000000.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp edge-port

Configure the port as an edge port.

Syntax

spanning-tree rstp edge-port <false|true>

default spanning-tree rstp edge-port

Parameters

Variable	Value
<false|true>	Enables or disables the port as an edge port.

Default

The default is disabled (false).

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp forward-time

Configures the RSTP forward delay for the bridge.

Syntax

spanning-tree rstp forward-time <400–3000>

default spanning-tree rstp forward-time

Parameters

Variable	Value
<400–3000>	Configures the RSTP forward delay for the bridge, in hundredths of a second.

Default

None

Command mode

Global Configuration mode

spanning-tree rstp group-stp enable

Enables or disables RSTP for a specific STG.

Syntax

spanning-tree rstp group-stp enable

default spanning-tree rstp group-stp enable

no spanning-tree rstp group-stp [enable]

Parameters

None

Default

None

Command mode

Global Configuration mode

spanning-tree rstp hello-time

Configure the hello-time delay for the bridge.

Syntax

spanning-tree rstp hello-time <100–1000>

default spanning-tree rstp hello-time

Parameters

Variable	Value
<100–1000>	Configures the hello-time for a port in one hundredths of a second.

Default

The default is 2.

Command mode

Global Configuration mode

spanning-tree rstp max-age

Assigns the RSTP maximum age time for the bridge

Syntax

spanning-tree rstp max-age <600–4000>

Parameters

Variable	Value
<600–4000>	Assigns the RSTP maximum age time for the bridge, in one hundredths of a second.

Default

None

Command mode

Global Configuration mode

spanning-tree rstp p2p

Specifies the point-to-point status of the LAN segment attached to this port.

Syntax

spanning-tree rstp p2p <auto|force-false|false-true>

default spanning-tree rstp p2p

Parameters

Variable	Value
<auto|force-false|false-true>	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.

Default

The default is auto.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp pathcost-type

Assigns the RSTP default pathcost version.

Syntax

spanning-tree rstp pathcost-type <bits16|bits32>

default spanning-tree rstp pathcost-type

Parameters

Variable	Value
<bits16|bits32>	Specifies the pathcost value.

Default

The default is 32 bits.

Command mode

Global Configuration mode

spanning-tree rstp port

Configure all RSTP parameters for a port.

Syntax

spanning-tree rstp port {slot/port} cost <1–200000000>

spanning-tree rstp port {slot/port} edge-port <false|true>

spanning-tree rstp port {slot/port} p2p <auto|force-false|false-true>

spanning-tree rstp port {slot/port} priority <0–240>

spanning-tree rstp port {slot/port} protocol-migration <false|true>

spanning-tree rstp port {slot/port} stp enable

default spanning-tree rstp port {slot/port} cost

default spanning-tree rstp port {slot/port} edge-port

default spanning-tree rstp port {slot/port} p2p

default spanning-tree rstp port {slot/port} priority

default spanning-tree rstp port {slot/port} protocol-migration

default spanning-tree rstp port {slot/port} stp

no spanning-tree rstp port {slot/port} stp enable

Parameters

Variable	Value
<0–240>	Specifies the four most significant bits of the port identifier. The values configured for port priority must be in steps of 16.
<1–200000000>	Specifies the cost value.
<auto|force-false|false-true>	A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.

Variable	Value
edge-port <false|true>	Enables or disables the port as an edge port.
port {slot/port}	Specifies the slot and port to configure.
protocol-migration <false|true>	Configures the protocol migration state of this port.

Default

The following list provides the command defaults:

- cost: 2000000
- edge-port: disabled (false)
- p2p: auto
- priority: 128
- protocol-migration: false
- stp: disabled

Command mode

Interface Configuration mode

spanning-tree rstp priority (globally)

Assigns the RSTP bridge priority.

Syntax

`spanning-tree rstp priority <0–61440>`

`default spanning-tree rstp priority`

Parameters

Variable	Value
<0–61440>	Assigns the RSTP bridge priority in a range of 0 to 61440 in steps of 4096.

Default

The default is 32768.

Command mode

Global Configuration mode

spanning-tree rstp priority (on a port)

Specifies the four most significant bits of the port identifier for a given spanning tree instance that can be modified independently for each spanning tree instance supported by the bridge.

Syntax

spanning-tree rstp priority <0–240>

default spanning-tree rstp priority

Parameters

Variable	Value
<0–240>	Specifies the four most significant bits of the port identifier. Assigns RSTP bridge priority in a range of 0–240. The values configured for port priority must be in steps of 16.

Default

The default is 128.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp protocol-migration

Enables or disables protocol migration for the port. If enabled, the port transmits BPDUs without instance information.

Syntax

spanning-tree rstp protocol-migration <false|true>

default spanning-tree rstp protocol-migration

Parameters

Variable	Value
<false|true>	Configures the protocol migration state of this port.

Default

The default is false.

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp stp

Enables STP on the port.

Syntax

spanning-tree rstp stp enable

default spanning-tree rstp stp

no spanning-tree rstp stp enable

Parameters

The default is disabled.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

spanning-tree rstp tx-holdcount

Assigns the RSTP transmit hold count.

Syntax

spanning-tree rstp tx-holdcount <1–10>

default spanning-tree rstp tx-holdcount

Parameters

Variable	Value
<1–10>	Assigns the RSTP transmit hold count.

Default

The default is 6.

Command mode

Global Configuration mode

spanning-tree rstp version

Configure the RSTP to set the RSTP configuration.

Syntax

`spanning-tree rstp version <rstp|stp-compatible>`

Parameters

Variable	Value
rstp version <*rstp*|*stp-compatible*>	Sets the version to RSTP or to STP compatible. The default is RSTP.

Default

The default is RSTP.

Command mode

Global Configuration mode

show spanning-tree status

View spanning-tree status information.

Syntax

`show spanning-tree status`

Parameters

None

Default

None

Command mode

Privileged EXEC mode

spoof-detect portlist enable

Configure the spoof detection to prevent an IP spoofing.

Syntax

spoof-detect [port {slot/port [-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	Enables spoof detection on the port.
port *{slot/port [-slot/port][,...]}*	Specifies the port list.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

subnet-vlan

Enable subnet-based VLAN on the port.

Syntax

subnet-vlan [port {slot/port[-slot/port][,...]}] [enable]

default subnet-vlan [port {slot/port[-slot/port][,...]}] [enable]

no subnet-vlan [port {slot/port[-slot/port][,...]}] [enable]

Parameters

Variable	Value
enable	Enables or disables subnet-based VLAN for the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is enabled.

Command mode

GigabitEthernet Interface Configuration mode

tagged-frames-discard

Discard tagged frames on the port.

Syntax

tagged-frames-discard [port {slot/port[-slot/port][,...]}] enable

default tagged-frames-discard [port {slot/port[-slot/port][,...]}] enable

no tagged-frames-discard [port {slot/port[-slot/port][,...]}] enable

Parameters

Variable	Value
enable	Discards tagged frames on the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration mode

untagged-frames-discard

Configure a tagged port to discard all untagged packets so that the frame is not classified into the default VLAN for the port.

Syntax

untagged-frames-discard [port {slot/port [-slot/port [,...]}]

Parameters

Variable	Value
port *{slot/port [-slot/port [,...]}*	Specifies the slots and ports that are to be changed.

Default

None

Command mode

GigabitEthernet Interface Configuration mode

untag-port-default-vlan

Untag the default VLAN on the port.

Syntax

untag-port-default-vlan [port {slot/port[-slot/port][,...]}] enable

default untag-port-default-vlan [port {slot/port[-slot/port][,...]}] enable

no untag-port-default-vlan [port {slot/port[-slot/port][,...]}] enable

Parameters

Variable	Value
enable	Untags the default VLAN for the port.
port *{slot/port[-slot/port][,...]}*	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

The default is disabled.

Command mode

GigabitEthernet Interface Configuration mode

vlan action

Perform the general VLAN operations to set a Quality of Service (QoS) level for the VLAN add and to change the name of a VLAN.

Syntax

vlan action <1-4084> {none|flushMacFdb|flushArp|flushIp| flushDynMemb|triggerRipUpdate|all}

Parameters

Variable	Value
none	Sets action to none.
flushArp	Sets action to flushMacFdb.
flushIp	Sets action to flushIp.
flushDynMemb	Sets action to flushDynMemb.
triggerRipUpdate	Sets action to triggerRipUpdate.
all	Sets action to all.

Default

None

Command mode

Global Configuration mode

vlan agetime

Configure the agetime for dynamic VLAN membership.

Syntax

vlan agetime <2–2084> <0–1000000>

default vlan agetime <2–2084>

Parameters

Variable	Value
<2–2084>	Specifies the VLAN ID.

Variable	Value
<0–1000000>	Specifies the agetime, in seconds.

Default

The default is 600 seconds.

Command mode

Global Configuration mode

vlan create

Configure VLANs to discard tag or untagged frames for a port.

Syntax

vlan create <2-4084> [name <WORD 0-64>] type {ipsubnet-mstprstp <0-63> {A.B.C.D/X} [color <0-32>]|port-mstprstp <0-63> [color <0-32>]|protocol-mstprstp <0-63> WORD<0-64>|srcmacmstprstp< 0-63>}

Parameters

Variable	Value
<2-4084>	Specifies the VLAN ID in the range of 2 to 4084.
name *WORD<0-64>*	Specifies the VLAN name in the range of 0–64. This parameter is optional. **Note:** Do not use the name Mgmt when you specify a name for the VLAN that you create. The VSP 9000 creates a management VLAN at boot up with the assigned name Mgmt. The show command does not show the management VLAN.
type ipsubnet-mstprstp *<0-63> <A.B.C.D/X> [color <0-32]*	Creates a VLAN by IP subnet: • *<0-63>* is the STP instance ID in the range of 0–63. • *A.B.C.D/X* is the subnet address or mask {a.b.c.d/x | a.b.c.d/x.x.x.x}. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.

Variable	Value
type port-mstprstp <*0-63*> *[color <0-32>]*	Creates a VLAN by port: • *0-63* is the STP instance ID from 0 to 63. • *color* <*0-32*> is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp <*0–63*> {appleTalk|decLat|decOther|ip|netBios|PPPoE|rarp|sna802dot2|snaEthernet2|vines|xns} [color <0-32>]	Creates a VLAN by protocol: • *0–63* is the STP instance ID. • appleTalk is the apple talk protocol. • decLat is the declat protocol. • decOther is the decother protocol. • ip is the Ip protocol. • netbios is the Netbios protocol. • PPPoE is the Point-to-Point Protocol Over Ethernet. • rarp is the Rarp protocol. • sna802dot2 is the Sna802dot2 protocol. • snaethernet2 is the Snaethernet2 protocol. • vines is the Vines protocol. • xns is the Xns protocol. • color <0-32> is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp <*0–63*> userDefined *{0x0000|<decimal value>}* [color] <*0-32*>] [encap {ethernet-ii|llc|snap}]	Creates a VLAN using a user defined protocol. • <*0-63*> is the STP instance ID in the range of 0–63. • *{0x0000|<decimal value>}* is the protocol ID in hexadecimal or decimal value. • color <0-32> is the color of the VLAN in the range of 0 to 32. • *encap* specifies the frame encapsulation header type.
type srcmac-mstprstp <*0-63*> [color <*0-32*>]	Creates a VLAN by source MAC address: • *0-63* is the STP instance ID in the range of 0–63. • color <0-32> is the color of the VLAN in the range of 0 to 32.

Default

None

Command mode

Global Configuration mode

vlan delete

Deletes a VLAN.

Syntax

vlan delete <2-4084>

no vlan <2-4084>

Parameters

Variable	Value
<2-4084>	

Default

None

Command mode

Global Configuration mode

vlan mac-address-entry

Configure the entries in the FDB to configure or modify the VLAN entries in the FDB.

Syntax

vlan mac-address-entry <1-4084> [aging-time <10–1000000>|flush|sync]

Parameters

Variable	Value
<1–4084>	Specifies the VLAN ID in the range of 1 to 4084.
aging-time *<10-1000000>*	Sets the FDB aging timer. **seconds** indicates the timeout period in seconds.
flush	Flushes the FDB.

Variable	Value
sync	Synchronizes the switch forwarding database with the forwarding database of the other aggregation switch.

Default

None

Command mode

Global Configuration mode

vlan mac-address-static

Configure the static members of a VLAN to set the VLAN static member parameters.

Syntax

vlan mac-address-static <1-4084> <0x00:0x00:0x00:0x00:0x00:0x00> {slot/port [-slot/port][,...]}

Parameters

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00>	Adds a static member to a VLAN bridge:
<1-4084>	Specifies the VLAN ID in the range of 1 to 4084.
{slot/port [-slot/port][,...]}	Specifies the slot and the port number.

Default

None

Command mode

Global Configuration mode

vlan members

Add or remove the ports in a VLAN to configure the ports in the VLAN.

Syntax

vlan members add <1-4084> {slot/port [-slot/port][,...]} [portmember|static|notallowed]

vlan members remove <1-4084> {slot/port [-slot/port][,...]} [portmember|static|notallowed]

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID.
portmember	Select the port type to port member.
static	Selects the port type to static.
notallowed	Selects the port type to not-allowed.
{slot/port [-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Global Configuration mode

vlan mlt

Add an MLT to a VLAN.

Syntax

vlan mlt <1-4084> <1–512>

Parameters

Variable	Value
<1-4084>	Specifies the VLAN ID.
<1–512>	Specifies the MLT ID.

Default

None

Command mode

Global Configuration mode

vlan srcmac

Add or remove a VLAN source MAC addresses to configure the source MAC address to a VLAN.

Syntax

vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>

no vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>

Parameters

Variable	Value
<0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the source MAC address.
<2-4084>	Specifies the VLAN ID in the range of 2–4084.

Default

None

Command mode

Global Configuration mode

vlan static-mcastmac

Adds VLAN static multicast MAC entries.

Syntax

vlan static-mcastmac <1–4084> [0x00:0x00:0x00:0x00:0x00:0x00] [{slot/port[-slot/port][,...]}] [mlt WORD<1–256>]

vlan static-mcastmac <1–4084> ports {slot/port[-slot/port][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]

default vlan static-mcastmac <1–4084> [0x00:0x00:0x00:0x00:0x00:0x00] [mlt WORD<1–256>]

default vlan static-mcastmac <1–4084> ports {slot/port[-slot/port] [,...]} [0x00:0x00:0x00:0x00:0x00:0x00]

no vlan static-mcastmac <1–4084> 0x00:0x00:0x00:0x00:0x00:0x00

no vlan static-mcastmac <1–4084> mlt WORD<1–256> [0x00:0x00:0x00:0x00:0x00:0x00]]

no vlan static-mcastmac <1–4084> ports {slot/port[-slot/port][,...]} [0x00:0x00:0x00:0x00:0x00:0x00]

Parameters

Variable	Value
0x00:0x00:0x00:0x00:0x00:0x00	Specifies the MAC address.
<1–256>	Specifies the MLT ID.
<1–4084>	Specifies the VLAN ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Default

None

Command mode

Global Configuration mode

Chapter 19: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.