Lenovo RackSwitch G8272

ISCLI—Industry Standard CLI Command Reference

for Lenovo Enterprise Network Operating System 8.4

Lenovo™

Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices* and *User Guide* documents on the Lenovo *Documentation* CD, and the *Warranty Information* document that comes with the product.

Second Edition (July 2017)

Contents

Preface

The *Lenovo RackSwitch G8272 ISCLI—Industry Standard CLI Command Reference for Lenovo Enterprise Network Operating System 8.4* describes how to configure and use the Enterprise NOS 8.4 software with your RackSwitch G8272 (referred to as G8272 throughout this document). This guide lists each command, together with the complete syntax and a functional description, from the IS Command Line Interface (ISCLI).

For documentation on installing the switches physically, see the *Lenovo Installation Guide* for your RackSwitch G8272. For details about configuration and operation of your G8272, see the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Who Should Use This Book

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1, “ISCLI Basics“, describes how to connect to the switch and access the information and configuration commands. This chapter provides an overview of the command syntax, including command modes, global commands and shortcuts.

Chapter 2, “Information Commands“, shows how to view switch configuration parameters.

Chapter 3, “Statistics Commands“, shows how to view switch performance statistics.

Chapter 4, “Configuration Commands“, shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Link Aggregation and more.

Chapter 5, “Operations Commands“, shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The commands describe how to activate or deactivate optional software features.

Chapter 6, “Boot Options“, describes the use of the primary and alternate switch images, how to load a new software image and how to reset the software to factory defaults.

Chapter 7, “Maintenance Commands“, shows how to generate and access a dump of critical switch state information, how to clear it and how to clear part or all of the forwarding database.

Appendix A, “Enterprise NOS System Log Messages“, shows a listing of syslog messages.

Appendix B, “Getting help and technical assistance“, lists the resources available from Lenovo to assist you.

Appendix C, “Notices“, displays Lenovo legal information.

“Index” includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1. *Typographic Conventions*

Typeface or Symbol	Meaning
`plain fixed-width text`	This type is used for names of commands, files, and directories used within the text. For example: View the `readme.txt` file. It also depicts on-screen computer output and prompts.
`bold fixed-width text`	This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example: **`show sys-info`**
bold body text	This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
italicized body text	This italicized type indicates book titles, special terms, or words to be emphasized.
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping`** *<IP address>* you enter **`ping`** *192.32.10.12*
braces **{}**	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`show portchannel {`***<1-144>***`|hash|information}`** you enter: **`show portchannel`** *<1-144>* or **`show portchannel hash`** or **`show portchannel information`**

Table 1. *Typographic Conventions (continued)*

Typeface or Symbol	Meaning
brackets **[]**	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **show interface ip [***<1-128>***]** you enter **show interface ip** or **show interface ip** *<1-128>*
vertical line **|**	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show portchannel {***<1-144>***|hash|information}** you must enter: **show portchannel** *<1-144>* or **show portchannel hash** or **show portchannel information**

Chapter 1. ISCLI Basics

Your RackSwitch G8272 is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

This guide describes the individual ISCLI commands available for the G8272.

The ISCLI provides a direct method for collecting switch information and performing switch configuration. Using a basic terminal, the ISCLI allows you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Industry Standard Command Line Interface (ISCLI) for the switch.

ISCLI Command Modes

The ISCLI has three major command modes listed in order of increasing privileges, as follows:

- **User EXEC mode**

  This is the initial mode of access. By default, password checking is disabled for this mode, on console.

- **Privileged EXEC mode**

  This mode is accessed from User EXEC mode. This mode can be accessed using the following command: **`enable`**

- **Global Configuration mode**

  This mode allows you to make changes to the running configuration. If you save the configuration, the settings survive a reload of the G8272. Several sub-modes can be accessed from the Global Configuration mode. For more details, see Table 2. This mode can be accessed using the following command: **`configure terminal`**

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode—all lower-privilege mode commands are accessible when using a higher-privilege mode.

The following table lists the ISCLI command modes.

Table 2. *ISCLI Command Modes*

Command Mode/Prompt	Command used to enter or exit
User EXEC `RS G8272>`	Default mode, entered automatically on console Exit: **`exit`** or **`logout`**
Privileged EXEC `RS G8272#`	Enter Privileged EXEC mode, from User EXEC mode: **`enable`** Exit to User EXEC mode: **`disable`** Quit ISCLI: **`exit`** or **`logout`**
Global Configuration `RS G8272(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: **`configure terminal`** Exit to Privileged EXEC: **`end`** or **`exit`**
Interface IP `RS G8272(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: **`interface ip`** *<1-128>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 2. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
Interface loopback `RS G8272(config-ip-loopback)#`	Enter Interface Loopback Configuration mode, from Global Configuration mode: **`interface loopback`** *<1-5>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Interface port `RS G8272(config-if)#`	Enter Port Configuration mode, from Global Configuration mode: **`interface port`** *<port alias or number>* Exit to Privileged EXEC mode: **`exit`** Exit to Global Configuration mode: **`end`**
Interface PortChannel `RS G8272(config-PortChannel)#`	Enter PortChannel Configuration mode, from Global Configuration mode: **`interface portchannel {`***<1-144>***`|lacp`** *<key>***`}`** Exit to Privileged EXEC mode: **`exit`** Exit to Global Configuration mode: **`end`**
VLAN `RS G8272(config-vlan)#`	Enter VLAN Configuration mode, from Global Configuration mode: **`vlan`** *<VLAN ID (1-4094)>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router OSPF `RS G8272(config-router-ospf)#`	Enter OSPF Configuration mode, from Global Configuration mode: **`router ospf`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router OSPFv3 `RS G8272(config-router-ospf3)#`	Enter OSPFv3 Configuration mode, from Global Configuration mode: **`ipv6 router ospf`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router BGP `RS G8272(config-router-bgp)#`	Enter BGP Configuration mode, from Global Configuration mode: **`router bgp`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 2. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
Router RIP `RS G8272(config-router-rip)#`	Enter RIP Configuration mode, from Global Configuration mode: **`router rip`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Route Map `RS G8272(config-route-map)#`	Enter Route Map Configuration mode, from Global Configuration mode: **`route-map`** *<1-255>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router VRRP `RS G8272(config-vrrp)#`	Enter VRRP Configuration mode, from Global Configuration mode: **`router vrrp`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
PIM Component `RS G8272(config-ip-pim-comp)#`	Enter Protocol Independent Multicast (PIM) Component Configuration mode, from Global Configuration mode: **`ip pim component`** *<1-2>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
IKEv2 Proposal `RS G8272(config-ikev2-prop)#`	Enter IKEv2 Proposal Configuration mode, from Global Configuration mode: **`ikev2 proposal`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
MLD Configuration `RS G8272(config-router-mld)#`	Enter Multicast Listener Discovery Protocol Configuration mode, from Global Configuration mode: **`ipv6 mld`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
MST Configuration `RS G8272(config-mst)#`	Enter Multiple Spanning Tree Protocol Configuration mode, from Global Configuration mode: **`spanning-tree mst configuration`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 2. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
OpenFlow Instance `RS G8272(config-openflow-instance)#`	Enter OpenFlow Instance Configuration mode, from Global Configuration mode: **`openflow instance`** *<1-2>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
VSI Database `RS G8272(conf-vsidb)#`	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: **`virt evb vsidb`** *<VSIDB number>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
EVB Profile `RS G8272(conf-evbprof)#`	Enter Edge Virtual Bridging VSI Type Profile Configuration mode, from Global Configuration mode: **`virt evb profile`** *<1-16>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
UFP Virtual Port Configuration `RS G8272(config_ufp_vport)#`	Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: **`ufp port`** *<port alias or number>* **`vport`** *<1-8>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Scheduler Job `RS G8272(config-job)#`	Enter Python Scripting Scheduler Job Configuration mode, from Global Configuration mode: **`scheduler job name`** *<job name>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
VXLAN Gateway `RS G8272(conf-nsx-gw)#`	Enter VXLAN Gateway Configuration mode, from Global Configuration mode: **`nwv nsx-gw`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`exit`**
FC Zone Configuration `RS G8272(config-zone)#`	Enter Fibre Channel Zone Configuration mode, from Global Configuration mode: **`zone name`** *<1-64 characters>* **`vlan`** *<VLAN ID (2-4094)>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 2. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
FC Zoneset Configuration `RS G8272(config-zoneset)#`	Enter Fibre Channel Zoneset Configuration mode, from Global Configuration mode: **`zoneset name`** *<1-64 characters>* **`vlan`** *<VLAN ID (2-4094)>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
FC Alias Configuration `RS G8272(config-fcalias)#`	Enter Fibre Channel FC Alias Configuration mode, from Global Configuration mode: **`fcalias name`** *<1-64 characters>* **`vlan`** *<VLAN ID (2-4094)>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
License Key Configuration `RS G8272(Software-Key)#`	Enter License Key Configuration mode, from User EXEC mode: **`software-key`** Exit to User EXEC mode: **`exit`**

Global Commands

Some basic commands are recognized throughout the ISCLI command modes. These commands are useful for obtaining online help, navigating through the interface, and for saving configuration changes.

For help on a specific command, type the command, followed by `help`.

Table 3. *Description of Global Commands*

Command	Action
?	Provides more information about a specific command or lists commands available at the current level.
list	Lists the commands available at the current level.
exit	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
copy running-config startup-config	Write configuration changes to non-volatile flash memory.
logout	Exit from the command line interface and log out.
traceroute	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **traceroute [{**<*hostname*>**|**<*IP address*>**}** **[**<*max-hops (1-32)*>**]** **[**<*msec-delay (1-4294967295)*>**]]** **[data-port|mgt-port]]** Where: o `hostname/IP address`: Sets the hostname or IP address of the target station. o `max-hops`: Sets the maximum distance to trace. o `msec-delay`: Sets the number of milliseconds to wait for the response. By default, the management port is used. To use a specific port, use the following options: o data port: **data-port** o management port: **mgt-port** **Note:** The DNS parameters must be configured if specifying hostnames.

Table 3. *Description of Global Commands*

Command	Action
ping	Use this command to verify station-to-station connectivity across the network. The format is as follows: **ping [{**<*hostname*>**|**<*IP address*>**} [**<*tries (0-4294967295)*>** [**<*msec-delay (0-4294967295)*>** [**<*length (0/32-65500/2080)*>** [**<*source IP address*>** [**<*ttl (1-255)*>** [**<*tos (0-255)*>** [dont-fragment]]]]]]]** **[data-port|mgt-port]]** Where: o **hostname/IP address**: Sets the hostname or IP address of the target station. o **tries**: Sets the number of attempts (optional). o **msec-delay**: Sets the number of milliseconds between attempts (optional). o **length**: Sets the ping request payload size (optional). o **source IP address**: Sets the IP source address for the IP packet (optional). o **ttl**: Sets the Time to live in the IP header. o **tos**: Sets the Type of Service bits in the IP header. o **dont-fragment**: Sets the *don't fragment* bit in the IP header (only for IPv4 addresses). By default, the management port is used. To use a specific port, use the following options: o data port: **data-port** o management port: **mgt-port** **Note:** The DNS parameters must be configured if specifying hostnames.

Table 3. *Description of Global Commands*

Command	Action
telnet	This command is used to form a Telnet session between the switch and another network device. The format is as follows: **telnet [{**<*hostname*>**|**<*IP address*>**}** **[**<*service port (1-65535)*>**]** **[data-port|mgt-port]]** Where: o hostname/IP address: Sets the target station. o port: Sets the logical Telnet port or service number. By default, the management port is used. To use a specific port, use the following options: o data port: **data-port** o management port: **mgt-port** **Note:** The DNS parameters must be configured if specifying hostnames.
show history	This command displays the last ten issued commands.
show who	Displays a list of users who are currently logged in.
show line	Displays a list of users who are currently logged in, in table format.

Command Line Interface Shortcuts

The following shortcuts allow you to enter commands quickly and easily.

CLI List and Range Inputs

For VLAN and port commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `vlan` command permits the following options:

```
RS G8272(config)# vlan 1,3,4094                 (access VLANs 1, 3, and 4094)
RS G8272(config)# vlan 1-20                     (access VLANs 1 through 20)
RS G8272(config)# vlan 1-5,90-99,4090-4094      (access multiple ranges)
RS G8272(config)# vlan 1-5,19,20,4090-4094      (access a mix of lists and ranges)
```

The numbers in a range must be separated by a dash: *<start of range>-<end of range>*

Multiple ranges or list items are permitted using a comma: *<range or item 1>*, *<range or item 2>*

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to access multiple ports with one command:

```
RS G8272(config)# interface port 1-4            (access ports 1 though 4)
```

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same mode. For example, consider the following full command and a valid abbreviation:

```
RS G8272(config)# show mac-address-table interface port 12
```

or:

```
RS G8272(config)# sh ma i p 12
```

Tab Completion

By entering the first letter of a command at any prompt and pressing **<Tab>**, the ISCLI displays all available commands or options that begin with that letter. Entering additional letters further refines the list of commands or options displayed. If only one command fits the input text when **<Tab>** is pressed, that command is supplied on the command line, waiting to be entered.

If multiple commands share the typed characters, when you press **<Tab>**, the ISCLI completes the common part of the shared syntax.

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the G8272. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- **user**

  Interaction with the switch is completely passive—nothing can be changed on the G8272. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.

- **oper**

  Operators can make temporary changes on the G8272. These changes are lost when the switch is rebooted. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reboot of the switch, operators cannot severely impact switch operation.

- **admin**

  Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G8272. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

Note: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies.

Table 4. *User Access Levels*

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	
Operator	The Operator can make temporary changes that are lost when the switch is rebooted. Operators have access to the switch management features used for daily switch operations.	
Administrator	The superuser Administrator has complete access to all command modes, information, and configuration commands on the RackSwitch G8272, including the ability to change both the user and administrator passwords.	`admin`

Note: With the exception of the "admin" user, access to each user level can be disabled by setting the password to an empty value.

Idle Timeout

By default, the switch will disconnect your Telnet session after ten minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes, or disabled when set to 0:

`system idle` *<0-60>*

Command mode: Global Configuration

Chapter 2. Information Commands

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

Table 5. *Information Commands*

Command Syntax and Usage
`show interface status` *<port alias or number>* Displays configuration information about the selected port(s), including: o Port alias and number o Port speed o Duplex mode (half, full, or, auto) o Flow control for transmit and receive (no, yes, or, both) o Link status (up, down, or, disabled) o Port description For details, see page 163. **Command mode:** All
`show interface trunk` *<port alias or number>* Displays port status information, including: o Port alias and number o Whether the port uses VLAN Tagging or not o Port VLAN ID (PVID) o Port description o VLAN membership o FDB Learning status o Flooding status For details, see page 164. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each port. For details, see page 165. **Command mode:** All
`show information-dump` Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

System Information

The information provided by each command option is briefly described in the following table, with pointers to where detailed information can be found.

Table 6. *System Information Options*

Command Syntax and Usage
dir [configs|images] Displays the configuration files and NOS images currently on the switch. o `configs` - displays only the configuration files currently on the switch o `images` - displays only the system images currently on the switch For more details, see page 35. **Command mode**: Privileged EXEC
show access user Displays configured user names and their status. **Command mode:** Privileged EXEC
show logging [messages] [severity *<0-7>***] [reverse] [|{include|exclude|section|begin|head** *<1-2000>***| |last** *<1-2000>***}]** Displays the current syslog configuration, followed by the most recent 2000 syslog messages. o `messages` displays the most recent 2000 syslog messages only o `severity` displays syslog messages of the specified severity level o `reverse` displays syslog messages starting with the most recent message o `|` displays syslog messages that match one of the following filters: • `include` displays syslog messages that match the specified expression • `exclude` displays syslog messages that don't match the specified expression • `section` displays syslog messages that match the specified section • `begin` displays syslog messages beginning from the first message that matches the specified expression • `head` displays the oldest syslog messages for the specified value • `last` displays the most recent syslog messages for the specified value For details, see page 48. **Command mode:** All

Table 6. *System Information Options (continued)*

Command Syntax and Usage
show sys-info Displays system information, including: o System date and time o Switch model name and number o Switch name and location o Time of last boot o MAC address of the switch management processor o IP address of management interface o Hardware version and part number o Software image file and version number o Configuration name o Log-in banner, if one is configured o Internal temperatures o Fan status o Power supply status For details, see page 46. **Command mode:** All
show software-key Displays information about the license keys currently installed on the switch. **Command mode**: All

The following command displays the configuration files and NOS images currently on the switch:

dir

Command mode: Privileged EXEC

```
images:
total 18528
-rw-r--r--    1 root     root      10038789 Jan  8 14:16 image1
-rw-r--r--    1 root     root       8932087 Jan  7 20:16 image2
-rw-r--r--    1 root     root            16 Jan  8 14:18 uboot-hdr


configs:
total 8
-rw-r--r--    1 root     root           342 Jan 11 14:43 conf1
-rw-r--r--    1 root     root          7637 Jan 11 14:43 conf2
```

CLI Display Information

These commands allow you to display information about the number of lines per screen displayed in the CLI.

Table 7. *CLI Display Information Options*

Command Syntax and Usage
`show terminal-length` Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled. **Command mode:** All
`show line console length` Displays the number of lines per screen displayed in the CLI by default for console sessions. A value of 0 means paging is disabled. **Command mode:** All
`show line vty length` Displays the number of lines per screen displayed in the CLI by default for Telnet and SSH sessions. A value of 0 means paging is disabled. **Command mode:** All

Error Disable and Recovery Information

These commands allow you to display information about the Error Disable and Recovery feature for interface ports.

Table 8. *Error Disable Information Options*

Command Syntax and Usage
`show errdisable information` Displays all Error Disable and Recovery information. **Command mode:** All
`show errdisable link-flap [information]` Displays ports that have been disabled due to excessive link flaps. **Command mode:** All
`show errdisable recovery` Displays a list ports with their Error Recovery status. **Command mode:** All
`show errdisable timers` Displays a list of active recovery timers, if applicable. **Command mode:** All

SNMPv3 System Information

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC2271 to RFC2276.

Table 9. *SNMPv3 Information Options*

Command Syntax and Usage
`show snmp-server v3` Displays all the SNMPv3 information. To view a sample, see page 45. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 41. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 42. **Command mode:** All
`show snmp-server v3 group` Displays information about the group, including the security model, user name and group name. To view a sample, see page 42. **Command mode:** All
`show snmp-server v3 notify` Displays the Notify table information. To view a sample, see page 44. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 43. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 44. **Command mode:** All

Table 9. *SNMPv3 Information Options (continued)*

Command Syntax and Usage
show snmp-server v3 user Displays User Security Model (USM) table information. To view the table, see page 39. **Command mode:** All
show snmp-server v3 view Displays information about view, subtrees, mask and type of view. To view a sample, see page 40. **Command mode:** All

SNMPv3 USM User Table Information

The User-based Security Model (USM) in SNMPv3 provides security services such as authentication and privacy of messages. This security model makes use of a defined set of user identities displayed in the USM user table. The following command displays SNMPv3 user information:

show snmp-server v3 user

Command mode: All

The USM user table contains the following information:

- the user name
- a security name in the form of a string whose format is independent of the Secuity Model
- an authentication protocol, which is an indication that the messages sent on behalf of the user can be authenticated
- the privacy protocol

```
Engine ID = 80:00:4F:4D:03:08:17:F4:8C:E8:00

usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
adminshaaes                     HMAC_SHA, AES PRIVACY
```

Table 10. *USM User Table Information Parameters*

Field	Description
User Name	A string representing the user name you can use to access the switch.
Protocol	Whether messages sent from this user are protected from disclosure using a privacy protocol. Enterprise NOS supports DES algorithm for privacy and two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table Information

The user can control and restrict the access allowed to a group to only a subset of the management information in the management domain that the group can access within each context by specifying the group's rights in terms of a particular MIB view for security reasons.

The following command displays the SNMPv3 View Table:

`show snmp-server v3 view`

Command mode: All

```
View Name            Subtree                 Mask           Type
-----------------    ------------------   --------------  --------
iso                  1.3                                  included
v1v2only             1.3                                  included
v1v2only             1.3.6.1.6.3.15                       excluded
v1v2only             1.3.6.1.6.3.16                       excluded
v1v2only             1.3.6.1.6.3.18                       excluded
```

Table 11. *SNMPv3 View Table Information Parameters*

Field	Description
View Name	Displays the name of the view.
Subtree	Displays the MIB subtree as an OID string. A view subtree is the set of all MIB object instances which have a common Object Identifier prefix to their names.
Mask	Displays the bit mask.
Type	Displays whether a family of `view subtrees` is included or excluded from the MIB view.

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

The vacmAccessTable maps a group name, security information, a context, and a message type, which could be the read or write type of operation or notification into a MIB view.

The View-based Access Control Model defines a set of services that an application can use for checking access rights of a group. This group's access rights are determined by a read-view, a write-view and a notify-view. The read-view represents the set of object instances authorized for the group while reading the objects. The write-view represents the set of object instances authorized for the group when writing objects. The notify-view represents the set of object instances authorized for the group when sending a notification.

The following command displays SNMPv3 access information:

`show snmp-server v3 access`

Command mode: All

```
Group Name Model   Level         ReadV      WriteV     NotifyV
---------- ------- ------------- ---------- ---------- ----------
v1v2grp    snmpv1  noAuthNoPriv iso        iso        v1v2only
admingrp   usm     authPriv     iso        iso        iso
```

Table 12. *SNMPv3 Access Table Information*

Field	Description
Group Name	Displays the name of group.
Model	Displays the security model used, for example, SNMPv1, or SNMPv2 or USM.
Level	Displays the minimum level of security required to gain rights of access. For example, `noAuthNoPriv`, `authNoPriv`, or `authPriv.`
ReadV	Displays the MIB view to which this entry authorizes the read access.
WriteV	Displays the MIB view to which this entry authorizes the write access.
NotifyV	Displays the Notify view to which this entry authorizes the notify access.

SNMPv3 Group Table Information

A group is a combination of security model and security name that defines the access rights assigned to all the security names belonging to that group. The group is identified by a group name.

The following command displays SNMPv3 group information:

show snmp-server v3 group

Command mode: All

```
All active SNMPv3 groups are listed below:
Sec Model  User Name                       Group Name
---------- ------------------------------ ------------------------------
snmpv1     v1v2only                       v1v2grp
usm        adminmd5                       admingrp
usm        adminsha                       admingrp
usm        adminshaaes                    admingrp
```

Table 13. *SNMPv3 Group Table Information Parameters*

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

SNMPv3 Community Table Information

The following command displays the SNMPv3 community table information stored in the SNMP engine:

show snmp-server v3 community

Command mode: All

```
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
trap1      public     v1v2only             v1v2trap
```

Table 14. *SNMPv3 Community Table Information Parameters*

Field	Description
Index	Displays the unique index value of a row in this table
Name	Displays the community string, which represents the configuration.
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information stored in the SNMP engine:

`show snmp-server v3 target-address`

Command mode: All

```
Name       Transport Addr                Port Taglist    Params
---------- ----------------------------- ---- ---------- ---------------
trap1      47.81.25.66                   162  v1v2trap   v1v2param
```

Table 15. *SNMPv3 Target Address Table Information Parameters*

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this `snmpTargetAddrEntry`.
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the `snmpTargetParamsTable`. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

show snmp-server v3 target-parameters

Command mode: All

```
Name            MP Model   User Name         Sec Model  Sec Level
--------------- ---------- ----------------- ---------- ------------
v1v2param       snmpv2c    v1v2only          snmpv1     noAuthNoPriv
```

Table 16. *SNMPv3 Target Parameters Table Information*

Field	Description
Name	Displays the locally arbitrary, but unique identifier associated with this `snmpTargeParamsEntry`.
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the `securityName`, which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an `inconsistentValue` error if an attempt is made to set this variable to a value for a security model the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify Table:

show snmp-server v3 notify

Command mode: All

```
Name                Tag
------------------- -------------------
v1v2trap            v1v2trap
```

Table 17. *SNMPv3 Notify Table Information*

Field	Description
Name	The locally arbitrary, but unique identifier associated with this `snmpNotifyEntry`.
Tag	This represents a single tag value which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

SNMPv3 Dump Information

The following command displays SNMPv3 information:

`show snmp-server v3`

Command mode: All

```
Engine ID = 80:00:4F:4D:03:08:17:F4:8C:E8:00

usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
adminshaaes                     HMAC_SHA, AES PRIVACY

vacmAccess Table:
Group Name Model   Level        ReadV      WriteV     NotifyV
---------- ------- ------------ ---------- ---------- ----------
v1v2grp    snmpv1  noAuthNoPriv iso        iso        v1v2only
admingrp   usm     authPriv     iso        iso        iso

vacmViewTreeFamily Table:
View Name            Subtree                    Mask            Type
-------------------- -------------------------- --------------  ---------
iso                  1                                          included
v1v2only             1                                          included
v1v2only             1.3.6.1.6.3.15                             excluded
v1v2only             1.3.6.1.6.3.16                             excluded
v1v2only             1.3.6.1.6.3.18                             excluded

vacmSecurityToGroup Table:
All active SNMPv3 groups are listed below:
Sec Model  User Name                       Group Name
---------- ------------------------------ ------------------------------
snmpv1     v1v2only                       v1v2grp
usm        adminmd5                       admingrp
usm        adminsha                       admingrp
usm        adminshaaes                    admingrp

snmpCommunity Table:
Index            Name       User Name            Tag
---------------- ---------- -------------------- ------------
trap1            public     v1v2only             v1v2trap

snmpNotify Table:
Name                 Tag
-------------------- --------------------
v1v2trap             v1v2trap

snmpTargetAddr Table:
Name             Transport Addr            Port Taglist      Params
---------------- ------------------------- ---- ------------ -------------
trap1            47.81.25.66               162  v1v2trap     v1v2param

snmpTargetParams Table:
Name                 MP Model User Name            Sec Model Sec Level
-------------------- -------- -------------------- --------- ------------
v1v2param            snmpv2c  v1v2only             snmpv1    noAuthNoPriv
```

General System Information

The following command displays system information:

`show sys-info`

Command mode: All

```
System Information at  3:49:06 Sun Jun 23, 2014
Time zone: No timezone configured
Daylight Savings Time Status: Disabled

Lenovo RackSwitch G8272

Switch has been up for 4 days, 3 hours, 24 minutes and 45 seconds.
Last boot:  0:25:13 Wed Jun 19, 2014 (reset from console)

MAC address: a8:97:dc:dd:ed:00    IP (If 1) address: 192.168.49.50
Management Port MAC Address: a8:97:dc:dd:ed:fe
Management Port IP Address (if 128): 10.241.31.134
Hardware Revision: 0
Hardware Part No:  00CJ066
Switch Serial No:  Y052MV49Y009
Manufacturing date: 14/40

MTM Value: 7159-HCV
ESN: MM01008

Software Version 8.4.1.0 (FLASH image1), active configuration.
Boot kernel version 8.4.1.0

USB Boot: disabled



Temperature CPU Local       : 29 C
Temperature Ambient         : 27 C
Temperature Hot Spot        : 38 C
Temperature Asic Max        : 55 C

System Warning at 85 C / Shutdown at 95 C / Set Point is 70 C

Fan 1 Module 1:  3865rpm  60pwm(23%) Front-To-Back
Fan 2 Module 1:  4176rpm  60pwm(23%) Front-To-Back
Fan 3 Module 2:  3843rpm  60pwm(23%) Front-To-Back
Fan 4 Module 2:  4063rpm  60pwm(23%) Front-To-Back
Fan 5 Module 3:  4134rpm  60pwm(23%) Front-To-Back
Fan 6 Module 3:  4299rpm  60pwm(23%) Front-To-Back
Fan 7 Module 4:  4084rpm  60pwm(23%) Front-To-Back
Fan 8 Module 4:  4383rpm  60pwm(23%) Front-To-Back

System Fan Airflow: Front-To-Back

Power Supply 1: Front-To-Back [DPS-460KB C]
Power Supply 2: Front-To-Back [DPS-460KB C]

  Power Faults: PS2-Pwr
    Fan Faults: None
Service Faults: Too-Few-PS
```

Note: The display of temperature will come up only if the temperature of any of the sensors exceeds the temperature threshold. There will be a warning from the software if any of the sensors exceeds this temperature threshold. The switch will shut down if the power supply overheats.

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- Software image file and version number, and configuration name.
- IP address of the management interface
- Hardware version and part number
- Log-in banner, if one is configured
- Internal temperatures
- Fan status
- Power supply status

Show Specific System Information

The following table lists commands used for displaying specific entries from the general system information screen.

Table 18. *Specific System Information Options*

Command Syntax and Usage
`show environment fan` Displays information about internal temperatures and fan status. **Command mode:** All
`show environment power` Displays information about power supply status. **Command mode:** All
`show version brief` Displays the software version number, image file and configuration name. For a sample output, see below. **Command mode:** All

Sample output for command **`show version brief`**:

```
Software Version 8.4.1.0 (FLASH image1), active configuration.
```

Displays the software version number, image file and configuration name.

Show Recent Syslog Messages

The following command displays system log messages:

`show logging [messages] [severity` *<0-7>***`] [reverse]`**

Command mode: All

```
Current syslog configuration:
  host 0.0.0.0 via MGT port, severity 7, facility 0
  host2 0.0.0.0 via MGT port, severity2 7, facility2 0
  console enabled
  severity level of console output 6
  severity level of write to flash 7
  syslogging all features
  Syslog source loopback interface not set


Nov  2  5:49:53 172.25.254.19 INFO    console: System log cleared by user
admin.
Nov  2  5:51:23 172.25.254.19 CRIT    system: Fan Mod 4 Removed
Nov  2  5:54:27 172.25.254.19 CRIT    system: **** MAX TEMPERATURE (61)
ABOVE FAIL THRESH ****
Nov  2  5:54:27 172.25.254.19 CRIT    system: **** PLATFORM THERMAL
SHUTDOWN ****
Nov  2  6:02:06 0.0.0.0 NOTICE  system: link up on management port MGT
Nov  2  6:02:06 0.0.0.0 INFO    system: booted version 0.0.0 from FLASH
image2, active configuration
Nov  2  6:02:09 0.0.0.0 NOTICE  system: SR SFP+ inserted at port 63 is
Approved
Nov  2  6:02:12 0.0.0.0 NOTICE  system: 1m DAC  inserted at port 64 is
Accepted
Nov  2  6:22:54 172.25.254.19 NOTICE  mgmt: admin(admin) login on Console
Nov  2  6:33:00 172.25.254.19 NOTICE  mgmt: admin(admin) idle timeout
from Console
```

Each syslog message has a severity level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition that the administrator is being notified of, as shown here.

- `EMERG` Indicates the system is unusable
- `ALERT` Indicates action should be taken immediately
- `CRIT` Indicates critical conditions
- `ERR` Indicates error conditions or errored operations
- `WARNING` Indicates warning conditions
- `NOTICE` Indicates a normal but significant condition
- `INFO` Indicates an information message
- `DEBUG` Indicates a debug-level message

The `severity` option filters only syslog messages with a specific severity level between 0 and 7, from `EMERG` to `DEBUG` correspondingly.

The `reverse` option displays the output in reverse order, from the newest entry to the oldest.

User Status

The following command displays user status information:

`show access user`

Command mode: All except User EXEC

```
Usernames:
  user     - enabled - offline
  oper     - disabled - offline
  admin    - Always Enabled - online 1 session
Current User ID table:
  1: name paul   , dis, cos user    , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

LDAP Information

The following command displays LDAP server configuration information:

`show ldap-server`

Command mode: All except User EXEC

- for LDAP configured in legacy mode:

```
Current LDAP settings:
 Primary LDAP Server (null) via MGT port
 Secondary LDAP Server (null) via MGT port
 Current LDAP server (null)
 LDAP port 389, Retries 3, Timeout 5, LDAP server OFF, Backdoor access
disabled
 LDAP domain name
 LDAP user attribute uid
```

- for LDAP configured in enhanced mode:

```
Current LDAP settings:
 LDAP server 1
   10.10.43.55:389 via MGT port
 LDAP server 2
   LDAPserver109:389 via DATA port
 LDAP server 3
    (null)
 LDAP server 4
    (null)
 LDAP Bind Mode Login Credentials
 LDAP Bind DN (null)
 Retries 3, Timeout 5, LDAP server OFF, Backdoor access disabled
 LDAP domain name
 LDAP attributes
   user attribute uid
   group attribute memberOf
   login attribute ibm-chassisRole
 LDAP group filter (null)
```

Layer 2 Information

The following commands display Layer 2 information:

Table 19. *Layer 2 Information Commands*

Command Syntax and Usage
show dot1x information Displays 802.1X Information. For details, see page 54. **Command mode:** All
show failover trigger *<1-8>* **information** Displays Layer 2 Failover information. For details, see page 61. **Command mode:** All
show hotlinks information Displays Hot Links information. For details, see page 63. **Command mode:** All
show layer2 information Dumps all Layer 2 switch information available (10K lines or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All
show lldp information Displays Link Layer Discovery Protocol (LLDP) information. For details, see page 64. **Command mode:** All
show portchannel information Displays the state of each port in the various Link Aggregation Groups (LAGs). For details, see page 80. **Command mode:** All

Table 19. *Layer 2 Information Commands (continued)*

Command Syntax and Usage
`show spanning-tree` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP) and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: o Priority o Hello interval o Maximum age value o Forwarding delay o Aging time You can also see the following port-specific STG information: o Port alias and priority o Cost o State For details, see page 71. **Command mode:** All
`show spanning-tree blockedports` Lists the ports blocked by each STP instance. **Command mode:** All
`show spanning-tree mst configuration` Displays the current MSTP settings. **Command mode:** All
`show spanning-tree mst` *<0-32>* **`[information]`** Displays Spanning Tree information for the specified instance. `0` is used for CIST. CIST bridge information includes: o Priority o Hello interval o Maximum age value o Forwarding delay o Root bridge information (priority, MAC address, path cost, root port) CIST port information includes: o Port number and priority o Cost o State For details, see page 78. **Command mode:** All

Table 19. *Layer 2 Information Commands (continued)*

Command Syntax and Usage
`show spanning-tree root` Displays root bridge ID for every spanning-tree instance and the path cost associated to it. For details, see page 77. **Command mode:** All
`show spanning-tree stp` *<1-128>* **`[information]`** Displays information about a specific Spanning Tree Group. For details, see page 72. **Command mode:** All
`show vlag` Displays vLAG Information. For details, see page 69. **Command mode:** All
`show vlan` Displays VLAN configuration information for all configured VLANs, including: o VLAN Number o VLAN Name o Status o Port membership of the VLAN For details, see page 81. **Command mode:** All

802.1X Information

The following command displays 802.1X information:

`show dot1x information`

Command mode: All

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
Guest VLAN status : disabled
Guest VLAN        : none
                                    Authenticator    Backend   Assigned
Port    Auth Mode    Auth Status      PAE State     Auth State   VLAN
-----  ------------  ------------  --------------  ---------- --------
*1     force-auth    unauthorized  initialize      initialize   none
*2     force-auth    unauthorized  initialize      initialize   none
*3     force-auth    unauthorized  initialize      initialize   none
```

The following table describes the IEEE 802.1X parameters.

Table 20. *802.1X Parameter Descriptions*

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: o `force-unauth` o `auto` o `force-auth`
Auth Status	Displays the current authorization status of the port, either `authorized` or `unauthorized`.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: o `initialize` o `disconnected` o `connecting` o `authenticating` o `authenticated` o `aborting` o `held` o `forceAuth`

Table 20. *802.1X Parameter Descriptions (continued)*

Parameter	Description
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: o `initialize` o `request` o `response` o `success` o `fail` o `timeout` o `idle`
Assigned VLAN	Displays corresponding VLAN associated with the port.

FDB Information

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

Note: The master forwarding database supports up to 128K MAC address entries on the MP per switch.

Table 21. *FDB Information Options*

Command Syntax and Usage
show mac-address-table Displays all entries in the Forwarding Database. **Command mode:** All
show mac-address-table all Displays all unicast and multicast entries in the Forwarding Database. **Command mode**: All
show mac-address-table address *<MAC address>* Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`. **Command mode:** All
show mac-address-table configured-static Displays all configured static MAC entries in the FDB. **Command mode:** All
show mac-address-table interface port *<port alias or number>* Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table multicast Displays all static multicast MAC entries in the FDB. For details, see page 57. **Command mode:** All
show mac-address-table portchannel *<1-144>* Displays all FDB entries for a particular Link Aggregation Group (LAG). **Command mode:** All
show mac-address-table private-vlan *<VLAN ID (2-4094)>* Displays all FDB entries on a single private VLAN. **Command mode:** All

Table 21. *FDB Information Options (continued)*

Command Syntax and Usage
show mac-address-table state {unknown|forward|trunk} Displays all FDB entries for a particular state. **Command mode:** All
show mac-address-table static Displays all static unicast MAC entries in the FDB. **Command mode:** All
show mac-address-table vlan *<VLAN ID (1-4094)>* Displays all FDB entries on a single VLAN. **Command mode:** All

FDB Multicast Information

The following commands display FDB multicast information.

Table 22. *Multicast FDB Information Options*

Command Syntax and Usage
show mac-address-table multicast Displays all Multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table multicast address *<MAC address>* Displays a single multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`. **Command mode:** All
show mac-address-table multicast interface port *<port alias or number>* Displays all multicast entries for a particular port. **Command mode:** All
show mac-address-table multicast vlan *<VLAN ID (1-4094)>* Displays all multicast entries on a single VLAN. **Command mode:** All

Show All FDB Information

The following command displays Forwarding Database information:

`show mac-address-table`

Command mode: All

```
Mac address Aging Time: 300

     MAC address       VLAN     Port    Trnk  State  Permanent  Openflow
  -----------------  --------  -------  ----  -----  ---------  --------
  00:90:fa:75:0e:c4       1    2              FWD                  N
  00:90:fa:75:0e:c8       1    14             FWD                  N
  a8:97:dc:d1:f8:00       1    14             FWD                  N
```

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the aggregation (TRK) state, the port field represents the Link Aggregation Group (LAG) number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination are listed under "Reference ports."

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to "Forwarding Database Maintenance" on page 725.

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the G8272.

Table 23. *LACP Information Options*

Command Syntax and Usage
show lacp Displays the current LCAP configuration. **Command mode:** All
show lacp aggregator *<aggregator ID>* Displays detailed information about the LACP aggregator. **Command mode:** All
show lacp information Displays a summary of LACP information. For details, see page 60. **Command mode:** All
show lacp information state {down|off|up} Displays a summary of LACP information for the interfaces that are down, off or up. **Command mode**: All
show interface port *<port alias or number>* **lacp [information]** Displays LACP information about the selected port. **Command mode:** All

Link Aggregation Control Protocol

The following command displays LACP information:

`show lacp information`

Command mode: All

```
port mode   adminkey operkey selected   prio  aggr trunk status minlinks
-------------------------------------------------------------------------
1    active 65535    65535   yes        32768 1    65     up    1
2    active 65535    65535   yes        32768 1    65     up    1
3    active 65535    65535   individual 32768 --   --    down   1
4    active 65535    65535   yes        32768 1    65     up    1
5    active 65535    65535   yes        32768 1    65     up    1
6    active 65535    65535   yes        32768 1    65     up    1
7    active 65535    65535   yes        32768 1    65     up    1
8    active 65535    65535   yes        32768 1    65     up    1
9    active 1000     1000    suspended  32768 --   --    down   1
10   active 1000     1000    suspended  32768 --   --    down   1
...
(*) LACP PortChannel is statically bound to the admin key
```

LACP dump includes the following information for each port in the G8272:

- `mode` Displays the port's LACP mode (active, passive or off).
- `adminkey` Displays the value of the port's *adminkey*.
- `operkey` Shows the value of the port's operational key.
- `selected` Indicates whether the port has been selected to be part of a Link Aggregation Group.
- `prio` Shows the value of the port priority.
- `aggr` Displays the aggregator associated with each port.
- `trunk` This value represents the LACP Link Aggregation Group (LAG) number.
- `status` Displays the status of LACP on the port (up or down).
- `minlinks` Displays the minimum number of active links in the LACP Link Aggregation Group (LAG).

Layer 2 Failover Information

The following commands display Layer 2 Failover information:

Table 24. *Layer 2 Failover Information Options*

Command Syntax and Usage
show failover trigger [information] Displays a summary of Layer 2 Failover information. For details, see page 61. **Command mode:** All
show failover trigger *<trigger number>* **[information]** Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

show failover trigger information

Command mode: All

```
Failover: On

Trigger 1 Manual Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
 17         Operational
Control State: Auto Controlled
Member      Status
---------   -----------
Physical ports
 1          Operational

Trigger 2: Disabled

Trigger 3: Disabled

Trigger 4: Disabled

Trigger 5: Disabled

Trigger 6: Disabled

Trigger 7: Disabled

Trigger 8: Disabled
```

A monitor port's Failover status is `Operational` only if all the following conditions hold true:

- Port link is up.
- If Spanning-Tree is enabled, the port is in the `Forwarding` state.
- If the port is a member of an LACP Link Aggregation Group (LAG), the port is aggregated.

If any of these conditions are not true, the monitor port is considered to be failed.

A control port is considered to be operational if the monitor trigger state is `Up`. Even if a port's link status is `Down`, Spanning-Tree status is `Blocking`, and the LACP status is `Not Aggregated`, from a teaming perspective the port status is `Operational`, since the trigger is `Up`.

A control port's status is displayed as `Failed` only if the monitor trigger state is `Down`.

Hot Links Information

The following command displays Hot Links information:

`show hotlinks information`

Command mode: All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
Hot Links BPDU flood: disabled
Hot Links FDB update: disabled
FDB update rate (pps): 200

Current Trigger 1 setting: enabled
name "Trigger 1", preempt enabled, fdelay 1 sec

Active state: None

Master settings:
port 1
Backup settings:
port 2
```

Hot Links information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

LLDP Information

The following commands display LLDP information.

Table 25. *LLDP Information Options*

Command Syntax and Usage
show lldp Displays the current Link Layer Discovery Protocol (LLDP) configuration. **Command mode:** All
show lldp information Displays all LLDP information. **Command mode:** All
show lldp port [*<port alias or number>***]** Displays LLDP information for all ports or a specific port. **Command mode:** All
show lldp port *<port alias or number>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specified port. **Command mode:** All
show lldp port *<port alias or number>* **vport** *<1-8>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specified virtual port on the selected port. **Command mode:** All
show lldp receive Displays information about the LLDP receive state machine. **Command mode:** All
show lldp remote-device [*<1-256>***|detail]** Displays information received from LLDP-capable devices. For more information, see page 65. **Command mode:** All
show lldp remote-device port *<port alias or number>* Displays information received from LLDP-capable devices for a specific port. A list of ports needs to be delimited by ',' and a range of ports delimited by '-'. **Command mode:** All
show lldp transmit Displays information about the LLDP transmit state machine. **Command mode:** All

LLDP Remote Device Information

The following command displays LLDP remote device information:

`show lldp remote-device`

Command mode: All

```
LLDP Remote Devices Information
Legend(possible values in DMAC column) :
NB   - Nearest Bridge          - 01-80-C2-00-00-0E
NnTB - Nearest non-TPMR Bridge - 01-80-C2-00-00-03
NCB  - Nearest Customer Bridge - 01-80-C2-00-00-00
Total number of current entries: 9

LocalPort|Index|Remote Chassis ID  |Remote Port        |Remote System Name|DMAC
---------|-----|-------------------|-------------------|------------------|----
1        | 1   | 00 00 c9 e5 47 e3 | 00-00-c9-e5-47-e3 |                  | NB
1        | 2   | 00 00 c9 e5 47 e3 | 00-00-c9-e5-47-e3 |                  | NnTB
2        | 3   | 00 90 fa 75 0e c5 | 00-90-fa-75-0e-c5 |                  | NB
14       | 4   | a8 97 dc d1 f8 00 | 60                |                  | NB
14       | 5   | a8 97 dc d1 f8 00 | 60                |                  | NnTB
15       | 6   | a8 97 dc d1 f8 00 | 80                |                  | NB
15       | 7   | a8 97 dc d1 f8 00 | 80                |                  | NnTB
18       | 8   | 00 90 fa 3d 48 49 | 00-90-fa-3d-48-49 |                  | NB
MGT      | 9   | 74 99 75 c5 08 00 | 6                 | G8052-54         | NB
```

LLDP remote device information provides a summary of information about remote devices connected to the switch. To view detailed information about a device, as shown below, follow the command with the index number of the remote device. To view detailed information about all devices, use the `detail` option.

```
Local Port Alias: 1
        Remote Device Index     : 15
        Remote Device TTL       : 99
        Remote Device RxChanges : false
        Chassis Type            : Mac Address
        Chassis Id              : 00-18-b1-33-1d-00
        Port Type               : Locally Assigned
        Port Id                 : 23
        Port Description        : 23

        System Name        :
        System Description : Lenovo RackSwitch G8296, Lenovo Networking
OS: version 8.2.0.3, Boot image: version 8.2.0.3
        System Capabilities Supported : bridge, router
        System Capabilities Enabled   : bridge, router

        Remote Management Address:
                Subtype             : IPv4
                Address             : 10.100.120.181
                Interface Subtype   : ifIndex
                Interface Number    : 128
                Object Identifier   :
```

Unidirectional Link Detection Information

The following commands display UDLD information:

Table 26. *UDLD Information Options*

Command Syntax and Usage
show udld Displays all UDLD information. **Command mode:** All
show interface port *<port alias or number>* **udld** Displays UDLD information about the selected port. **Command mode:** All

UDLD Port Information

The following command displays UDLD information for the selected port:

show interface port *<port alias or number>* **udld**

Command mode: All

```
UDLD information on port 1
Port enable administrative configuration setting: Enabled
Port administrative mode: normal
Port enable operational state: link up
Port operational state: advertisement
Port bidirectional status: bidirectional
Message interval: 15
Time out interval: 5
Neighbor cache: 1 neighbor detected

   Entry #1
   Expiration time: 31 seconds
   Device Name:
   Device ID: 00:da:c0:00:04:00
   Port ID: 1
```

UDLD information includes the following:

- Status (enabled or disabled)
- Mode (normal or aggressive)
- Port state (link up or link down)
- Bi-directional status (unknown, unidirectional, bidirectional, TX-RX loop, neighbor mismatch)

802.1x Discovery Information

The following commands display 802.1x information:

Table 27. *802.1x Discovery Information Options*

Command Syntax and Usage
show interface port *<port alias or number>* **dot1x** Displays 802.1x information about the selected port. **Command mode:** All
show dot1x Displays all 802.1x information. **Command mode:** All
show dot1x *<port alias or number>* Displays 802.1x information for specified port. **Command mode:** All

802.1x Port Information

The following command displays 802.1x information for the selected port:

show interface port *<port alias or number>* **dot1x**

Command mode: All

```
                  Quiet  Tx    Max  Supp    Server ReAuth ReAuth  VLAN
Port Auth Mode  Period Period Req Timeout Timeout Status Period Assign
---- ---------- ------ ------ --- ------- ------- ------ ------ ------
G    force-auth 60     30     2   30      30      off    3600   off
1    force-auth 60     30     2   30      30      off    3600   off
--------------------------------------------------------------------------
G - Global port configuration
```

802.1x port display shows information about the selected port and the peer to which the link is connected.

OAM Discovery Information

The following commands display OAM information:

Table 28. *OAM Discovery Information Options*

Command Syntax and Usage
show interface port *<port alias or number>* **oam** Displays OAM information about the selected port. **Command mode:** All
show oam Displays all OAM information. **Command mode:** All

OAM Port Information

The following command displays OAM information for the selected port:

show interface port *<port alias or number>* **oam**

Command mode: All

```
OAM information on port 1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

Remote port information:
Mode active
MAC address 00:da:c0:00:04:00
Stable Yes
State valid Yes
Evaluating No
```

OAM port display shows information about the selected port and the peer to which the link is connected.

vLAG Information

The following commands display Virtual Link Aggregation Group (vLAG) information:

Table 29. *vLAG Information Options*

Command Syntax and Usage
show vlag Displays the current vLAG configuration. **Command mode:** All
show vlag adminkey *<1-65535>* Displays vLAG LACP information. **Command mode:** All
show vlag adminkey *<1-65535>* **information** Displays all vLAG LACP information. **Command mode:** All
show vlag information Displays all vLAG information. **Command mode:** All
show vlag isl Displays vLAG Inter-Switch Link (ISL) information. **Command mode:** All
show vlag peer-gateway Displays the current state of the vLAG peer gateway. For details, see page 70. **Command mode**: All
show vlag portchannel *<1-72>* Displays vLAG static Link Aggregation Group (LAG) information. **Command mode:** All
show vlag portchannel *<1-72>* **information** Displays all vLAG static Link Aggregation Group (LAG) information. **Command mode**: All

vLAG Aggregation Information

The following command displays vLAG information for the Link Aggregation Group (LAG):

`show vlag portchannel` *<1-72>*

Command mode: All

```
vLAG is enabled on trunk 13
Protocol - Static
Current settings: enabled
    ports:  13
Current L2 trunk hash settings:
    smac dmac
Current L3 trunk hash settings:
    sip dip
Current ingress port hash: disabled
Current L4 port hash: disabled
Current FCoE trunk hash settings:
    sid did
```

vLAG Peer Gateway Information

The following command displays the current state of the vLAG peer gateway.

`show vlag peer-gateway`

Command mode: All

```
Current peer gateway state: disabled
```

vLAG VRRP Information

The following command displays vLAG related VRRP information:

`show vlag vrrp`

Command mode: All

```
vLAG VRRP mode: Active
vLAG related VRRP information:
   1: vrid   1, local role master, peer role backup
  10: vrid   1, local role backup, peer role backup
 100: vrid   1, local role backup, peer role master
```

```
vLAG VRRP mode: Passive
vLAG related VRRP information:
   1: vrid   1, local role master, peer role init
  10: vrid   1, local role backup, peer role init
 100: vrid   1, local role backup, peer role init
```

Spanning Tree Information

The following command displays Spanning Tree information:

`show spanning-tree`

Command mode: All

```
Max PVRST Instances: 128
Pvst+ compatibility mode enabled

---------------------------------------------------------------------
Spanning Tree Group 1: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8002 34:40:b5:40:55:00        0       0    2     20     15

Prev Root:               Port        Replaced at
 0000 00:00:00:00:00:00  0           NA

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging   Topology Change Counts
              32770      2      20      15     300                  7

    Port      Prio    Cost    State  Role Designated Bridge      Des Port    Type
------------- ---- ---------- -----  ---- ---------------------- -------- ----------
51             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8033        P2P
52             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8034        P2P
53             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8035        P2P
54             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8036        P2P
55             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8037        P2P
56             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8038        P2P
57             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     8039        P2P
58             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     803a        P2P
59             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     803b        P2P
60             128      2000!  FWD   DESG 8002-34:40:b5:40:55:00     803c        P2P
! = Automatic path cost.
...
```

RSTP Information

The following command displays RSTP information:

`show spanning-tree stp` *<1>* **`information`**

Command mode: All

```
Spanning Tree Group 1: On (RSTP)
VLANs:  1 10 4095

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8000 00:25:03:49:29:00        0       0    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging   Topology Change Counts
              32768      2      20      15     300                   1

Port        Prio Cost State Role Designated Bridge      Des Port  Type
----------- ---- ---- ----- ---- ---------------------- -------- ------
1    (pc12) 128  490!+ FWD  DESG 8000-00:25:03:49:29:00   8026     P2P
2    (pc12) 128  490!+ FWD  DESG 8000-00:25:03:49:29:00   8026     P2P
3    (pc12) 128  490!+ FWD  DESG 8000-00:25:03:49:29:00   8026     P2P
4    (pc12) 128  490!+ FWD  DESG 8000-00:25:03:49:29:00   8026     P2P
MGT  0      0          FWD  *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) spanning tree mode, with IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP), as alternatives.

The following port-specific information is also displayed:

Table 30. *PVRST/RSTP/MSTP Port Parameter Descriptions*

Parameter	Description
Priority (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The Port Path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field can be one of the following: Discarding (DISC), Learning (LRN), or Forwarding (FWD).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`) or Backup (`BKUP`).

Table 30. *PVRST/RSTP/MSTP Port Parameter Descriptions (continued)*

Parameter	Description
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The Designated Port field shows the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P or SHARED.

PVRST Information

The following command displays PVRST information:

`show spanning-tree stp` *<1-128>* **`information`**

Command mode: All

```
Spanning Tree Group 1: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 8001 a8:97:dc:03:d5:00      490       1    2     20     15

Prev Root:               Port        Replaced at
 8001 a8:97:dc:d2:12:00  0           16:33:08  3- 3-2016

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging   Topology Change Counts
              32769      2      20      15     300                  8

    Port      Prio    Cost    State  Role Designated Bridge      Des Port    Type
------------ ---- ---------- -----  ---- ---------------------- -------- ----------
1     (pc1)    128       490!+ FWD   ROOT 8001-a8:97:dc:03:d5:00     8042         P2P
2     (pc1)    128       490!+ FWD   ROOT 8001-a8:97:dc:03:d5:00     8042         P2P
3     (pc1)    128       490!+ FWD   ROOT 8001-a8:97:dc:03:d5:00     8042         P2P
4     (pc1)    128       490!+ FWD   ROOT 8001-a8:97:dc:03:d5:00     8042         P2P
11             128      2000!  FWD   DESG 8001-a8:97:dc:d2:12:00     800b         P2P
13             128      2000!  FWD   DESG 8001-a8:97:dc:d2:12:00     800d         P2P
14             128      2000!  FWD   DESG 8001-a8:97:dc:d2:12:00     800e         P2P
16             128      2000!  FWD   DESG 8001-a8:97:dc:d2:12:00     8010         P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

You can configure the switch software to use the IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP) or PerVLAN Rapid Spanning Tree Protocol (PVRST).

The following port-specific information is also displayed:

Table 31. *RSTP/MSTP/PVRST Port Parameter Descriptions*

Parameter	Description
Prio (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port Path Cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The State field can be one of the following: Discarding (`DISC`), Learning (`LRN`), Forwarding (`FWD`) or Disabled (`DSB`).

Table 31. *RSTP/MSTP/PVRST Port Parameter Descriptions (continued)*

Parameter	Description
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (DESG), Root (ROOT), Alternate (ALTN), Backup (BKUP) or Disabled (DSB).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P or SHARED.

Spanning Tree Bridge Information

The following command displays Spanning Tree bridge information:

`show spanning-tree bridge`

Command mode: All

```
STG       Priority    Hello     MaxAge    FwdDel    Protocol  VLANs
------    --------    ------    ------    ------    --------  -----
1         32768       2         20        15        PVRST     1
2         32768       2         20        15        PVRST     2
128       32768       2         20        15        PVRST     4095
```

`show spanning-tree vlan` *<VLAN ID (1-4094)>* **`bridge`**

Command mode: All

```
Vlan       Priority     Hello     MaxAge         FwdDel         Protocol
------     --------     ------    ------         ------         --------
1          32768        2         20             15             MSTP
```

Table 32. *Bridge Parameter Descriptions*

Parameter	Description
VLAN	VLANs that are part of the Spanning Tree Group
Priority	The bridge priority parameter controls which bridge on the network will become the STP root bridge. The lower the value, the higher the priority.
Hello	The hello time parameter specifies, in seconds, how often the bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding state to learning state and from learning state to forwarding state.
Protocol	The STP protocol run by the Spanning Tree Group.

Spanning Tree Root Information

The following command displays information about the root bridge ID for every spanning-tree instance and the path cost associated to it:

`show spanning-tree root`

Command mode: All

```
Instance   Root ID                Path-Cost Hello MaxAge FwdDel Root Port
---------- --------------------- --------- ----- ------ ------ ---------
1          8001 08:17:f4:32:95:00 0         2     20     15             0
3          8003 08:17:f4:32:95:00 0         2     20     15             0
6          8001 08:17:f4:fb:d8:00 20000     2     20     15            27
17         8011 08:17:f4:32:95:00 0         2     20     15             0
```

Table 33. *Bridge Parameter Descriptions*

Parameter	Description
Instance	Spanning Tree instance
Root ID	Indicates the root switch bridge priority and MAC address.
Path-Cost	The port path cost is used to help determine the designated port for a segment.
Hello	The hello time parameter specifies, in seconds, how often the bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding state to learning state and from learning state to forwarding state.
Root Port	The elected root port for the STP instance (port used to reach the root switch).

Multiple Spanning Tree Information

The following command displays Multiple Spanning Tree (MSTP) information:

`show spanning-tree mst` *<0-32>* **`information`**

Command mode: All

```
Mstp Digest: 0x9f71e12a07f4e3004fe0ce1f241a7b66

------------------------------------------------------------------
Spanning Tree Group 5: On (MSTP)
VLANs MAPPED:  5
VLANs:  5

Current Root:            Path-Cost  Port
 0000 a8:97:dc:88:c9:00        0       0

Parameters:  Priority  Aging   Topology Change Counts
                  0     300                  1

    Port   Prio  Cost  State  Role Designated Bridge      Des Port  Type
---------- ---- ------ -----  ---- ---------------------- -------- --------
1  (pc105) 128   156!+  FWD   DESG 0000-a8:97:dc:88:c9:00  80e8    P2P
2  (pc105) 128   156!+  FWD   DESG 0000-a8:97:dc:88:c9:00  80e8    P2P
4          128   500!   FWD   DESG 0000-a8:97:dc:88:c9:00  800a    P2P,edge
22 (pc105) 128   156!+  FWD   DESG 0000-a8:97:dc:88:c9:00  80e8    P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

In addition to seeing Common Internal Spanning Tree (CIST) status, you can view the following CIST bridge information:

Table 34. *CIST Parameter Descriptions*

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.

Table 34. *CIST Parameter Descriptions (continued)*

Parameter	Description
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding state to learning state and from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is `20`.

The following port-specific CIST information is also displayed:

Table 35. *CIST Parameter Descriptions*

Parameter	Description
Prio (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (`DISC`), Learning (`LRN`) or Forwarding (`FWD`).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`), Backup (`BKUP`), Disabled (`DSB`) or Master (`MAST`).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are `AUTO`, `P2P` or `SHARED`.

Link Aggregation Group (LAG) Information

The following command displays Link Aggregation Group (LAG) information:

`show portchannel information`

Command mode: All

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  1: STG  1 forwarding
  2: STG  1 forwarding
```

When LAGs are configured, you can view the state of each port in the various LAGs.

Note: If Spanning Tree Protocol on any port in the LAG is set to `forwarding`, the remaining ports in the LAG will also be set to `forwarding`.

VLAN Information

The following commands display VLAN information:

Table 36. *VLAN Information Options*

Command Syntax and Usage
show vlan Displays the current VLAN configuration. **Command mode:** All
show vlan *<VLAN ID (1-4094)>* Displays the current configuration for the specified VLAN. **Command mode:** All
show vlan private-vlan [type] Displays Private VLAN information. o `type` lists only the VLAN type for each private VLAN: community, isolated or primary **Command mode:** All
show vlan information Displays information about all VLANs, including: o VLAN number and name o VLAN statistics o Port membership o VLAN status (enabled or disabled) o Protocol VLAN status o Spanning Tree membership o Private VLAN information o Flooding settings o VMAP configuration **Command mode:** All
show vlan *<VLAN ID (1-4094)>* **information** Displays information only about the specified VLAN. **Command mode:** All
show protocol-vlan *<protocol number (1-8)>* Displays Protocol VLAN information. **Command mode:** All

The following command displays VLAN information:

`show vlan`

Command mode: All

```
VLAN                Name                 Status            Ports
----  --------------------------------  ------  -------------------------
1     Default VLAN                       ena     1-49 50 51 52 53 54
2     VLAN 2                             ena     empty
3     VLAN 3                             ena     empty
4095  Mgmt VLAN                          ena     MGT

Primary  Secondary  Type             Ports                 vPorts
-------  ---------  ---------------  ----------------  ----------------
2                   primary          empty
         3          community        empty
```

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN
- Protocol VLAN information (if available)
- Private VLAN information (if available)

Layer 3 Information

The following commands display Layer 3 information:

Table 37. *Layer 3 Information Commands*

Command Syntax and Usage
show ikev2 Displays IKEv2 information. For more information options, see page 130. **Command mode:** All
show interface ip Displays IP interface Information. For details, see page 125. **Command mode:** All
show [ip] arp Displays Address Resolution Protocol (ARP) information. For details, see page 90. **Command mode:** All
show ip bgp Displays Border Gateway Protocol (BGP) information. For details, see page 97. **Command mode**: All
show ip bootp-relay Displays the current parameters for the BOOTP Relay broadcast domain. **Command mode:** All
show ip dhcp snooping Displays DHCP Snooping information. For details, see page 134. **Command mode:** All
show ip dns Displays the current Domain Name System settings. **Command mode:** All
show ip ecmp Displays ECMP static route information. For details, see page 115. **Command mode**: All
show ip gateway *<1-4>* Displays the current gateway settings. **Command mode:** All
show ipv6 gateway6 {*<1>***|***<4>***}** Displays the current IPv6 default gateway configuration. **Command mode**: All

Table 37. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
`show ip igmp` Displays IGMP Information. For more IGMP information options, see page 116. **Command mode**: All
`show ip information` Displays all IP information. **Command mode:** All
`show ip interface brief` Displays IP Information. For details, see page 128. IP information, includes: o IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. o Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status o IP forwarding settings, network filter settings, route map settings **Command mode:** All
`show ipv6 interface` *<interface number>* Displays IPv6 interface information. For details, see page 126. **Command mode:** All
`show ip match-address [`*<1-256>***`]`** Displays the current the Network Filter configuration. **Command mode:** All
`show ip mroute` Displays the current IP multicast routes. **Command mode:** All
`show ip nat` Displays NAT status information. For details, see page 147. **Command mode:** All
`show ipv6 mld` Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see page 121. **Command mode**: All
`show ipv6 neighbors` Displays IPv6 Neighbor Cache information. For more information options, see page 113. **Command mode**: All

Table 37. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
`show ip ospf information` Displays the OSPF information. For details, see page 98. **Command mode**: All
`show ipv6 ospf information` Displays OSPFv3 information. For more OSPFv3 information options, see page 104. **Command mode**: All
`show ip pim component [`*<1-2>***`]`** Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see page 135. **Command mode:** All
`show ipv6 pmtu [`*<destination IPv6 address>***`]`** Displays IPv6 Path MTU information. For details, see page 127. **Command mode:** All
`show ip policy` Displays the current routing policy information. **Command mode:** All
`show ip prefix-policy` Displays the current Prefix Policy Table configuration. **Command mode**: All
`show ipv6 prefix` Displays IPv6 Neighbor Discovery prefix information. For details, see page 114. **Command mode**: All
`show ip rip` Displays the current Routing Information Protocol (RIP) configuration. For details, see page 109. **Command mode**: All
`show ip route` Displays all routes configured on the switch. For details, see page 88. **Command mode:** All
`show ipv6 route` Displays IPv6 routing information. For more information options, see page 111. **Command mode**: All

Table 37. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
show ip routing Displays the current IP forwarding settings. **Command mode:** All
show ip slp information Displays Service Location Protocol (SLP) information. **Command mode**: All
show ip slp directory-agents Displays SLP Directory Agent (DA) information. **Command mode**: All
show ip slp user-agents Displays SLP User Agent (UA) information. **Command mode**: All
show ip tenant [info] *<1-30>* Displays tenant information. **Command mode**: All
show ip vrrp information Displays VRRP information. For details, see page 123. **Command mode:** All
show ipsec manual-policy Displays information about manual key management policy for IP security. For more information options, see page 132. **Command mode:** All
show layer3 Dumps all Layer 3 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data before issuing the dump commands. **Command mode:** All
show layer3 igmp-groups Displays the total number of IGMP groups that are registered on the switch. **Command mode:** All
show layer3 ipmc-groups Displays the total number of current IP multicast (IPMC) groups that are registered on the switch. **Command mode:** All

IP Routing Information

Using the commands listed in the following table, you can display all or a portion of the IP routes currently held in the switch.

Table 38. *Route Information Options*

Command Syntax and Usage
show ip route [all] Displays all routes configured in the switch. For more information, see page 88. **Command mode:** All
show ip route address *<IP address>* Displays a single route by destination IP address. **Command mode:** All
show ip route ecmphash Displays the current ECMP hashing mechanism. **Command mode:** All
show ip route gateway *<IP address>* Displays routes to a single gateway. **Command mode:** All
show ip route interface *<interface number>* Displays routes on a single interface. **Command mode:** All
show ip route port *<port alias or number>* Displays routes on a single port. **Command mode:** All
show ip route static Displays static routes configured on the switch. **Command mode:** All
show ip route tag {address|bgp|broadcast|fixed|martian| |multicast|ospf|rip|static} Displays routes of a single tag. For a description of IP routing tags, see Table 40 on page 88. **Command mode:** All
show ip route type {broadcast|direct|indirect|local| |martian|multicast} Displays routes of a single type. For a description of IP routing types, see Table 39 on page 88. **Command mode:** All

Show All IP Route Information

The following command displays IP route information:

`show ip route`

Command mode: All

```
Mgmt routes:
Status code: * - best
    Destination         Mask          Gateway        Type      Tag    Metric If
  --------------- --------------- --------------- --------- --------- ------ ---
* 192.168.50.0    255.255.255.0   192.168.50.50   direct    fixed             128
* 192.168.50.50   255.255.255.255 192.168.50.50   local     addr              128
* 192.168.50.255  255.255.255.255 192.168.50.255  broadcast broadcast         128

Data routes:
Status code: * - best
    Destination         Mask          Gateway        Type      Tag    Metric If
  --------------- --------------- --------------- --------- --------- ------ ---
* 127.0.0.0       255.0.0.0       0.0.0.0         martian   martian
* 224.0.0.0       224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.0       240.0.0.0       0.0.0.0         multicast addr
* 255.255.255.255 255.255.255.255 255.255.255.255 broadcast broadcast
```

The following table describes the `Type` parameters.

Table 39. *IP Routing Type Parameters*

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the `Gateway` address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the `Tag` parameters.

Table 40. *IP Routing Tag Parameters*

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the RackSwitch G8272.
addr	The address belongs to one of the switch's IP interfaces.

Table 40. *IP Routing Tag Parameters (continued)*

Parameter	Description
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP).
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 42 on page 92), VLAN, age and port for the address.

Table 41. *ARP Information Options*

Command Syntax and Usage
show [ip] arp [all] Displays all ARP entries. including: o IP address and MAC address of each entry o Address status flag o The VLAN and port to which the address belongs o The elapsed time (in seconds) since the ARP entry was learned For more information, see page 91. **Command mode:** All
show ip arp data Displays all data ARP entries. **Command mode:** All
show [ip] arp find *<IP address>* Displays a single ARP entry by IP address. **Command mode:** All
show ip arp inspection Displays the current Dynamic ARP Inspection (DAI) configuration settings. For details, see page 93. **Command mode:** All
show [ip] arp interface port *<port alias or number>* Displays the ARP entries on a single port. **Command mode:** All
show ip arp management Displays all management ARP entries. **Command mode:** All
show [ip] arp reply Displays the ARP entries for the switch's IP interfaces. **Command mode:** All

Table 41. *ARP Information Options (continued)*

Command Syntax and Usage
show [ip] arp static Displays all static ARP entries. **Command mode:** All
show [ip] arp vlan *<VLAN ID (1-4095)>* Displays the ARP entries on a single VLAN. **Command mode:** All

ARP Address List Information

The following command displays owned ARP address list information:

show [ip] arp reply

Command mode: All

```
    IP address        IP mask        MAC address     VLAN Pass-Up
  --------------- --------------- -----------------  ---- -----
  1.1.1.1         255.255.255.255 08:17:f4:62:64:00     1
  2.2.2.2         255.255.255.255 08:17:f4:62:64:00     1
  46.0.0.1        255.255.255.255 08:17:f4:62:64:00  4094
  3.3.3.20        255.255.255.255 08:17:f4:62:64:00     3
```

Show All ARP Entry Information

The following command displays ARP information:

show [ip] arp

Command mode: All

```
Mgmt ARP entries:

Total number of Mgmt ARP entries : 2
    IP address    Flags    MAC address     VLAN   Age Port
  --------------- ----- ----------------- ------  --- ----
  10.241.32.185    P    a8:97:dc:de:00:fe   4095      MGT
  10.241.32.254         74:99:75:d3:04:00   4095  151 MGT

Data ARP entries:

Current ARP configuration:
  rearp 5
No static ARP configured.

Total number data ARP entries : 1
    IP address    Flags    MAC address     VLAN   Age Port
  --------------- ----- ----------------- ------  --- ----
  192.168.49.50    P    a8:97:dc:de:00:00      1
```

The `Port` field shows the target port of the ARP entry.

The `Flags` field is interpreted as follows:

Table 42. *ARP Flag Parameters*

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

Dynamic ARP Inspection Information

The following commands display Dynamic ARP Inspection (DAI) information:

Table 43. *Dynamic ARP Inspection Information Options*

Command Syntax and Usage
show ip arp inspection Displays the current DAI configuration settings. **Command mode:** All
show ip arp inspection interfaces [*<port alias or number>***]** Displays the current DAI configuration settings for the selected interfaces. **Command mode:** All
show ip arp inspection vlan [*<VLAN ID (1-4094)>***]** Displays the current DAI configuration settings for the selected VLANs. **Command mode:** All

show ip arp inspection interfaces [*<port alias or number>***]**

Command mode: All

```
Interface  Trust State
---------  -----------
1          Trusted
2          Trusted
3          Untrusted
4          Untrusted
...
```

show ip arp inspection vlan [*<VLAN ID (1-4094)>***]**

Command mode: All

```
Vlan  Configuration
----  -------------
   2  Enabled
```

BGP Information

The following commands display BGP information:

Table 44. *BGP Peer Information Options*

Command Syntax and Usage
show ip bgp aggregate-address [*<1-16>***]** Displays the current BGP aggregation configuration. **Command mode:** All
show ip bgp information Displays the BGP routing table. See page 97 for a sample output. **Command mode:** All
show ip bgp neighbor [*<1-192>***]** Displays the current BGP peer configuration. **Command mode:** All
show ip bgp neighbor advertised-routes Displays all BGP advertised routes to all neighbors. **Command mode**: All
show ip bgp neighbor *<1-192>* **advertised-routes** Displays all BGP advertised routes to a specific peer. **Command mode**: All
show ip bgp neighbor group Displays BGP group information. See page 96 for a sample output. **Command mode:** All
show ip bgp neighbor information Displays BGP peer information. See page 95 for a sample output. **Command mode:** All
show ip bgp neighbor *<1-192>* **information** Displays BGP peer information for a specific peer. **Command mode:** All
show ip bgp neighbor *<1-192>* **redistribute** Displays BGP neighbor redistribution. **Command mode:** All

Table 44. *BGP Peer Information Options (continued)*

Command Syntax and Usage
show ip bgp neighbor *<1-192>* **routes** Displays BGP peer routes. **Command mode:** All
show ip bgp neighbor summary Displays peer summary information such as AS, message received, message sent, up/down or state. See page 97 for a sample output. **Command mode:** All

BGP Peer Information

Following is an example of the information provided by the following command:

show ip bgp neighbor information

Command mode: All

```
BGP Peer Information:
Static Peers:
  1: 3.5.0.3         , version 4, TTL 255, TTL Security hops 0
    Remote AS: 10000, Local AS: 10000, Link type: IBGP
    Remote router ID: 3.3.3.3,    Local router ID: 5.5.5.5
    next-hop-self disabled
    RR client disabled
    BGP status: established, Old status: established
    Total received packets: 4321, Total sent packets: 4309
    Received updates: 12, Sent updates: 0
    Keepalive: 60, Holdtime: 180, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 1
```

BGP Group Information

Following is an example of the information provided by the following command:

`show ip bgp neighbor group`

Command mode: All

```
BGP Group Information:
Local router ID: 1.1.1.2, Local AS: 100
Group 1:
    Name: toG82642007
    Addr: 192.168.128.0    Mask: 255.255.255.248
    Remote AS list: 200
    Dynamic Peers Limit: 8
    Dynamic Peers in established state: 1
 Dynamic Peers of this group:
 97: 192.168.128.4, Group: 1 (toG82642007), TTL 1
    Remote AS: 200, Local AS: 100, Link type: EBGP
    Remote router ID: 2.2.1.2, Local router ID: 1.1.1.2
    Configured Version: 4
    Negotiated Version: 4
    Total path attribute out: 0
    In Total Messages: 74
    Out Total Messages: 74
    In Updates: 0
    Out Updates: 0
    Established Time: 01:12:36
    MinAdvTime: 00:01:00
    Configured holdtime: 00:03:00
    Negotiated holdtime: 00:03:00
    Configured keepalive 00:01:00
    Negotiated keepalive 00:01:00
    In Update Last Time: 00:00:00
    Out Update Last Time: 00:14:32
    Last Send Time: 01:26:54
    Last Received Time: 01:26:54
    In-rmap list count: 0
    Out-rmap list count: 0
...
```

BGP Summary Information

Following is an example of the information provided by the following command:

`show ip bgp neighbor summary`

Command mode: All

```
BGP Peer Summary Information:
      Peer         V    AS     MsgRcvd  MsgSent Up/Down   State
   -------------- - -------- -------- -------- -------- ----------
1: 205.178.23.142  4      142      113      121 00:00:28 established
2: 205.178.15.148  0      148        0        0 never    connect
```

Dump BGP Information

Following is an example of the information provided by the following command:

`show ip bgp information [`<*IPv4 network*> <*IPv4 mask*>**`] [longer_prefix]`**

Command mode: All

```
Status codes: * valid, > best, = multipath, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network         Mask            Next Hop        Metric LcPrf  Wght  Path
--------------- --------------- --------------- ------ ----- ----- ------
*> 1.1.1.0      255.255.255.0   0.0.0.0                          0      ?
*> 10.100.100.0 255.255.255.0   0.0.0.0                          0      ?
*> 10.100.120.0 255.255.255.0   0.0.0.0                          0      ?
```

The IPv4 network and mask options restrict the output to a specific network in the BGP routing table.

OSPF Information

The following commands display OSPF information:

Table 45. *OSPF Information Options*

Command Syntax and Usage
show interface ip *<1-128>* **ospf** Displays the current OSPF settings for the specified IP interface. **Command mode:** All
show ip ospf area *<0-19>* Displays OSPF settings for a particular area index. **Command mode:** All
show ip ospf area information [*<0-19>***]** Displays area information for all areas or a particular area index. **Command mode:** All
show ip ospf area-range *<1-16>* Displays the current OSPF summary range settings. **Command mode:** All
show ip ospf area-virtual-link *<1-3>* Displays the current OSPF virtual link settings. **Command mode:** All
show ip ospf area-virtual-link information Displays information about all the configured virtual links. **Command mode:** All
show ip ospf general-information Displays general OSPF information. See page 100 for a sample output. **Command mode:** All
show ip ospf host *<1-128>* Displays the current OSPF host entries. **Command mode:** All
show ip ospf host information Displays OSPF host configuration information. **Command mode:** All
show ip ospf information Displays the OSPF information. **Command mode:** All

Table 45. *OSPF Information Options (continued)*

Command Syntax and Usage
show ip ospf interface [<*IP interface number*>**]** Displays OSPF information for all IP interfaces or a particular interface. See page 100 for a sample output. **Command mode:** All
show ip ospf interface loopback [<*1-5*>**]** Displays OSPF information for all loopback interfaces or a particular loopback interface. See page 101 for a sample output. **Command mode:** All
show ip ospf interface port [<*port alias or number*>**]** Displays OSPF information for all ports or a particular port. For details, see page 101. **Command mode:** All
show ip ospf neighbor Displays the status of all the current neighbors. **Command mode:** All
show ip ospf redistribute Displays the current OSPF redistribute settings. **Command mode:** All
show ip ospf routes Displays OSPF routing table. See page 101 for a sample output. **Command mode:** All
show ip ospf summary-range <*0-19*> Displays the list of summary ranges belonging to non-NSSA areas. **Command mode:** All
show ip ospf summary-range-nssa <*0-19*> Displays the list of summary ranges belonging to NSSA areas. **Command mode:** All

OSPF General Information

The following command displays general OSPF information:

show ip ospf general-information

Command mode: All

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                  2 are >=INIT state,
                                  2 are >=EXCH state,
                                  2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
        Area Id : 0.0.0.0
        Authentication : none
        Import ASExtern : yes
        Number of times SPF ran : 8
        Area Border Router count : 2
        AS Boundary Router count : 0
        LSA count : 5
        LSA Checksum sum : 0x2237B
        Summary : noSummary
```

OSPF Interface Information

The following command displays OSPF interface information:

show ip ospf interface *<interface number>*

Command mode: All

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
   Router ID 10.10.10.1, State DR, Priority 1
   Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
   Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
   Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
                Poll interval 0, Transit delay 1
   Neighbor count is 1   If Events 4, Authentication type none
```

OSPF Loopback Information

The following command displays OSPF information for a particular loopback interface. If no parameter is supplied, it displays OSPF information for all the loopback interfaces:

`show ip ospf interface loopback` *<1-5>*

Command mode: All

```
Ip Address 123.123.123.1, Area 0.0.0.0, Passive interface, Admin Status UP
   Router ID 1.1.1.1, State Loopback, Priority 1
   Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay 1
   Neighbor count is 0   If Events 1, Authentication type none
```

OSPF Port Information

The following command displays OSPF information for a particular port. If no parameter is supplied, it displays OSPF information for all the ports:

`show ip ospf interface port` *<port alias or number>*

Command mode: All

```
Ip Address 10.241.39.82, Area 0.0.0.0, Admin Status UP
   Router ID 1.1.1.1, State Waiting, Priority 1
   Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay 1
   Neighbor count is 0   If Events 1, Authentication type none
```

OSPF Information Route Codes

The following command displays OSPF route information:

`show ip ospf routes`

Command mode: All

```
Codes: IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
 IA 10.10.0.0/16 via 200.1.1.2
 IA 40.1.1.0/28 via 20.1.1.2
 IA 80.1.1.0/24 via 200.1.1.2
 IA 100.1.1.0/24 via 20.1.1.2
 IA 140.1.1.0/27 via 20.1.1.2
 IA 150.1.1.0/28 via 200.1.1.2
 E2 172.18.1.1/32 via 30.1.1.2
 E2 172.18.1.2/32 via 30.1.1.2
 E2 172.18.1.3/32 via 30.1.1.2
 E2 172.18.1.4/32 via 30.1.1.2
 E2 172.18.1.5/32 via 30.1.1.2
 E2 172.18.1.6/32 via 30.1.1.2
 E2 172.18.1.7/32 via 30.1.1.2
 E2 172.18.1.8/32 via 30.1.1.2
```

OSPF Database Information

The following commands display OSPF Database information:

Table 46. *OSPF Database Information Options*

Command Syntax and Usage
show ip ospf database Displays all the Link State Advertisements (LSAs). **Command mode:** All
show ip ospf database advertising-router *<router ID (IP address)>* Takes advertising router as a parameter. Displays all the LSAs in the LS database that have the advertising router with the specified router ID, for example: `20.1.1.1`. **Command mode:** All
show ip ospf database area *<0-19>* Displays LS database information for the specified OSPF area. **Command mode:** All
show ip ospf database asbr-summary [advertising-router *<router ID (IP address)>***|link-state-id** *<link state ID (IP address)>***|self]** Displays ASBR summary LSAs. The usage of this command is as follows: o `asbr-summary advertising-router 20.1.1.1` displays ASBR summary LSAs having the advertising router 20.1.1.1. o `asbr-summary link-state-id 10.1.1.1` displays ASBR summary LSAs having the link state ID 10.1.1.1. o `asbr-summary self` displays the self advertised ASBR summary LSAs. o `asbr-summary` with no parameters displays all the ASBR summary LSAs. **Command mode:** All
show ip ospf database database-summary Displays the following information about the LS database in a table format: o Number of LSAs of each type in each area. o Total number of LSAs for each area. o Total number of LSAs for each LSA type for all areas combined. o Total number of LSAs for all LSA types for all areas combined. No parameters are required. **Command mode:** All
show ip ospf database external [advertising-router *<router ID (IP address)>***|link-state-id** *<link state ID (IP address)>***|self]** Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. **Command mode:** All

Table 46. *OSPF Database Information Options (continued)*

Command Syntax and Usage
show ip ospf database network [advertising-router *<router ID (IP address)>* **|link-state-id** *<link state ID (IP address)>* **|self]** Displays the network (type 2) LSAs with detailed information of each field of the LSA. **Command mode:** All
show ip ospf database nssa [advertising-router *<router ID (IP address)>* **|link-state-id** *<link state ID (IP address)>* **|self]** Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. **Command mode:** All
show ip ospf database router [advertising-router *<router ID (IP address)>* **|link-state-id** *<link state ID (IP address)>* **|self]** Displays the router (type 1) LSAs with detailed information of each field of the LSAs. **Command mode:** All
show ip ospf database self Displays all the self-advertised LSAs. No parameters are required. **Command mode:** All
show ip ospf database summary [advertising-router *<router ID (IP address)>* **|link-state-id** *<link state ID (IP address)>* **|self]** Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs. **Command mode:** All

OSPFv3 Information

The following commands display OSPFv3 information:

Table 47. *OSPFv3 Information Options*

Command Syntax and Usage
show ipv6 ospf area *<area index (0-2)>* Displays the OSPFv3 area information. **Command mode:** All
show ipv6 ospf areas Displays the OSPFv3 Area Table. **Command mode:** All
show ipv6 ospf area-range *<1-16>* Displays the current OSPFv3 summary range settings. **Command mode:** All
show ipv6 ospf area-range information Displays OSPFv3 summary ranges. **Command mode:** All
show ipv6 ospf area-virtual-link *<1-3>* Displays the current OSPFv3 virtual link settings. **Command mode:** All
show ipv6 ospf area-virtual-link information Displays information about all the configured virtual links. **Command mode:** All
show ipv6 ospf border-routers Displays OSPFv3 routes to an ABR or ASBR. **Command mode:** All
show ipv6 ospf host *<1-128>* Displays the current OSPFv3 host entries. **Command mode:** All
show ipv6 ospf host information Displays OSPFv3 host configuration information. **Command mode:** All
show ipv6 ospf information Displays all OSPFv3 information. To view a sample display, see page 106. **Command mode:** All

Table 47. *OSPFv3 Information Options (continued)*

Command Syntax and Usage
show ipv6 ospf interface [<*interface number*>**]** Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see page 106. **Command mode:** All
show ipv6 ospf neighbor [<*nbr router-ID (IP address)*>**]** Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors. **Command mode:** All
show ipv6 ospf redist-config <*1-128*> Displays the current OSPFv3 redistribution configuration for the specified entry. **Command mode**: All
show ipv6 ospf redist-config information Displays OSPFv3 redistribution information to be applied to routes learned from the route table. **Command mode:** All
show ipv6 ospf request-list [<*nbr router-ID (IP address)*>**]** Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors. **Command mode:** All
show ipv6 ospf retrans-list [<*nbr router-ID (IP address)*>**]** Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors. **Command mode:** All
show ipv6 ospf routes Displays OSPFv3 routing table. To view a sample display, see page 108. **Command mode:** All
show ipv6 ospf summary-prefix <*1-16*> Displays the current OSPFv3 AS-external range. **Command mode**: All
show ipv6 ospf summary-prefix information Displays the OSPFv3 external summary-address configuration information. **Command mode:** All

OSPFv3 Information Dump

The following command displays OSPFv3 information:

show ipv6 ospf information

Command mode: All

```
Router Id: 1.0.0.1           ABR Type: Standard ABR
 SPF schedule delay: 5 secs  Hold time between two SPFs: 10 secs
 Exit Overflow Interval: 0   Ref BW: 100000       Ext Lsdb Limit: none
 Trace Value: 0x00008000     As Scope Lsa: 2      Checksum Sum: 0xfe16
 Passive Interface: Disable
 Nssa Asbr Default Route Translation: Disable
 Autonomous System Boundary Router
 Redistributing External Routes from connected, metric 10, metric type
 asExtType1, no tag set
 Number of Areas in this router  1
                        Area    0.0.0.0
     Number of interfaces in this area is 1
     Number of Area Scope Lsa: 7     Checksum Sum: 0x28512
     Number of Indication Lsa: 0     SPF algorithm executed: 2 times
```

OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

show ipv6 ospf interface

Command mode: All

```
Ospfv3 Interface Information

Interface Id: 1      Instance Id: 0      Area Id: 0.0.0.0
Local Address: fe80::222:ff:fe7d:5d00    Router Id: 1.0.0.1
Network Type: BROADCAST  Cost: 1         State: BACKUP

Designated Router Id: 2.0.0.2      local address:
fe80::218:b1ff:fea1:6c01

Backup Designated Router Id: 1.0.0.1      local address:
fe80::222:ff:fe7d:5d00

Transmit Delay: 1 sec    Priority: 1     IfOptions: 0x0
Timer intervals configured:
Hello: 10,  Dead: 40,  Retransmit: 5
Hello due in 6 sec
Neighbor Count is: 1,  Adjacent neighbor count is: 1
Adjacent with neighbor 2.0.0.2
```

OSPFv3 Database Information

The following commands display OSPFv3 Database information:

Table 48. *OSPFv3 Database Information Options*

Command Syntax and Usage
show ipv6 ospf database [detail|hex] Displays all the Link State Advertisements (LSAs). **Command mode:** All
show ipv6 ospf database as-external [detail|hex] Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database inter-prefix [detail|hex] Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database inter-router [detail|hex] Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database intra-prefix [detail|hex] Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database link [detail|hex] Displays Link LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database network [detail|hex] Displays Network LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database nssa [detail|hex] Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database router [detail|hex] Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information. **Command mode:** All

OSPFv3 Route Codes Information

The following command displays OSPFv3 route information:

show ipv6 ospf routes

Command mode: All

```
Dest/           NextHp/          Cost  Rt. Type     Area
Prefix-Length   IfIndex
3ffe::10:0:0:0  fe80::290:69ff    30   interArea    0.0.0.0
/80              fe90:b4bf /vlan1
3ffe::20:0:0:0  fe80::290:69ff    20   interArea    0.0.0.0
/80              fe90:b4bf /vlan1
3ffe::30:0:0:0  ::         /vlan2 10   intraArea    0.0.0.0
/80
3ffe::60:0:0:6  fe80::211:22ff    10   interArea    0.0.0.0
/128             fe33:4426 /vlan2
```

Routing Information Protocol

The following commands display information:

Table 49. *Routing Information Protocol Options*

Command Syntax and Usage
show ip rip Displays the current RIP configuration. **Command mode:** All
show ip rip interface [*<IP interface number>***|port** *<port alias or number>***]** Displays the current RIP interface configuration. For more information, see page 110. **Command mode:** All
show ip rip redistribute Displays the current RIP route redistribute configuration. **Command mode:** All
show ip rip routes Displays RIP routes. For more information, see page 110. **Command mode:** All

RIP Routes Information

The following command displays RIP route information:

`show ip rip routes`

Command mode: All

```
>> IP Routing#

30.1.1.0/24 directly connected
3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2
```

This table contains all dynamic routes learned through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain locally configured static routes.

RIP Interface Information

The following command displays RIP user information:

`show ip rip interface` *<interface number>*

Command mode: All

```
RIP USER CONFIGURATION :
        RIP: ON, update 30
        RIP on Interface    49 : 101.1.1.10,      enabled
        version 2, listen enabled, supply enabled, default none
        poison disabled, split horizon enabled, trigg enabled, mcast enabled, metric 1
        auth none, key none
```

IPv6 Routing Information

The following table discribes the IPv6 Routing information options.

Table 50. *IPv6 Routing Information Options*

Command Syntax and Usage
show ipv6 route Displays all IPv6 routing information. For more information, see page 112. **Command mode:** All
show ipv6 route address *<IPv6 address>* Displays a single route by destination IPv6 address. **Command mode:** All
show ipv6 route gateway *<IPv6 gateway address>* Displays routes to a single gateway. **Command mode:** All
show ipv6 route interface *<interface number>* Displays routes on a single interface. **Command mode:** All
show ipv6 route static Displays the current static route configuration. **Command mode**: All
show ipv6 route summary Displays a summary of IPv6 routing information, including inactive routes. **Command mode:** All
show ipv6 route type {connected|static|ospf} Displays routes of a single type. For a description of IP routing types, see Table 39 on page 88. **Command mode:** All

IPv6 Routing Table Information

The following command displays IPv6 routing information:

show ipv6 route

Command mode: All

```
IPv6 Routing Table  -  3 entries
Codes : C - Connected, S - Static
        O - OSPF
        D - Data Gateway from RA
        M - Management Gateway
        N - Management Gateway from RA

S ::/0 [1/20]
via 2001:2:3:4::1, Interface 2

C 2001:2:3:4::/64 [1/1]
via ::, Interface 2

C fe80::20f:6aff:feec:f701/128 [1/1]
```

Note that the first number inside the brackets represents the metric and the second number represents the preference for the route.

IPv6 Neighbor Cache Information

The following commands display IPv6 Neighbor Cache information:

Table 51. *IPv6 Neighbor Cache Information Options*

Command Syntax and Usage
show ipv6 neighbors Displays all IPv6 Neighbor Cache entries. For more information, see page 113. **Command mode:** All
show ipv6 neighbors find *<IPv6 address>* Displays a single IPv6 Neighbor Cache entry by IP address. **Command mode:** All
show ipv6 neighbors interface port *<port alias or number>* Displays IPv6 Neighbor Cache entries on a single port. **Command mode:** All
show ipv6 neighbors static Displays static IPv6 Neighbor Cache entries. **Command mode:** All
show ipv6 neighbors vlan *<VLAN ID (1-4094)>* Displays IPv6 Neighbor Cache entries on a single VLAN. **Command mode:** All

IPv6 Neighbor Cache Information

The following command displays a summary of IPv6 Neighbor Cache information:

show ipv6 neighbors

Command mode: All

```
IPv6 Address              Age  Link-layer Addr   State     IF  VLAN Port
------------------------- ---- ----------------- --------- --- ---- ----
2001:2:3:4::1             10   00:50:bf:b7:76:b0 Reachable 2   1       1
fe80::250:bfff:feb7:76b0   0   00:50:bf:b7:76:b0 Stale     2   1       2
```

IPv6 Neighbor Discovery Prefix Information

The following command displays a summary of IPv6 Neighbor Discovery prefix information:

`show ipv6 prefix`

Command mode: All

```
Codes: A  - Address , P - Prefix-Advertisement
       D  - Default , N - Not Advertised
      [L] - On-link Flag is set
      [A] - Autonomous Flag is set

AD 10:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime 604800
P 20:: 64 [LA] Valid lifetime 200 , Preferred lifetime 100
```

Neighbor Discovery prefix information includes information about all configured prefixes.

The following command displays IPv6 Neighbor Discovery prefix information for an interface:

`show ipv6 prefix interface` *<interface number>*

Command mode: All

ECMP Static Route Information

The following command displays Equal Cost Multi-Path (ECMP) route information:

`show ip ecmp`

Command mode: All

```
Current ecmp static routes:
Destination     Mask            Gateway         If    GW Status
--------------- --------------- --------------- ---- -----------
10.10.1.1       255.255.255.255 100.10.1.1        1    up
                                200.20.2.2        1    down

10.20.2.2       255.255.255.255 10.233.3.3        1    up
10.20.2.2       255.255.255.255 10.234.4.4        1    up
10.20.2.2       255.255.255.255 10.235.5.5        1    up

ECMP health-check ping interval: 1
ECMP health-check retries number: 3
ECMP Hash Mechanism: dipsip
```

ECMP route information shows the status of each ECMP route configured on the switch.

IGMP Information

The following commands display IGMP information:

Table 52. *IGMP Multicast Group Information Commands*

Command Syntax and Usage
show ip igmp Displays the current IGMP configuration parameters. **Command mode:** All
show ip igmp filtering Displays current IGMP Filtering parameters. **Command mode:** All
show ip igmp groups Displays information for all multicast groups. For details, see page 119. **Command mode:** All
show ip igmp groups address *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
show ip igmp groups detail *<IP address>* Displays details about an IGMP multicast group, including source and timer information. **Command mode:** All
show ip igmp groups interface port *<port alias or number>* Displays all IGMP multicast groups on a single port. **Command mode:** All
show ip igmp groups portchannel *<1-144>* Displays all IGMP multicast groups on a single Link Aggregation Group (LAG). **Command mode:** All
show ip igmp groups vlan *<VLAN ID (1-4094)>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
show ip igmp ipmcgrp Displays information for all IPMC groups. For details, see page 120. **Command mode:** All

Table 52. *IGMP Multicast Group Information Commands (continued)*

Command Syntax and Usage
`show ip igmp mrouter [dynamic|interface port` *<port alias or number>* **`| |portchannel`** *<1-144>* **`|static]`** Displays information for all Mrouters, all dynamic/static Mrouter ports installed or Mrouter ports specific to a specified interface/portchannel. **Command mode**: All
`show ip igmp mrouter information` Displays IGMP Multicast Router information. For details, see page 119. **Command mode:** All
`show ip igmp mrouter vlan` *<VLAN ID (1-4094)>* Displays IGMP Multicast Router information for the specified VLAN. **Command mode:** All
`show ip igmp profile` *<1-16>* Displays information about the current IGMP filter. **Command mode:** All
`show ip igmp querier port` *<port alias or number>* Displays IGMP Querier information for a particular port. **Command mode:** All
`show ip igmp querier vlan` *<VLAN ID (1-4094)>* Displays IGMP Querier information for a particular VLAN. For details, see page 118. **Command mode:** All
`show ip igmp relay` Displays IGMP Relay information. **Command mode:** All
`show ip igmp snoop` Displays IGMP Snooping information. **Command mode:** All
`show ip igmp snoop igmpv3` Displays the current IGMPv3 Snooping configuration. **Command mode:** All

IGMP Querier Information

The following command displays IGMP Querier information for a particular VLAN:

`show ip igmp querier vlan` *<VLAN ID (1-4094)>*

Command mode: All

```
Current IGMP Querier information:
 IGMP Querier information for vlan 1:
 Other IGMP querier - none
 Switch-querier enabled, current state: Querier
 Switch-querier type: Ipv4, address 1.1.1.1,
 Switch-querier general query interval: 125 secs,
 Switch-querier max-response interval: 100 'tenths of secs',
 Switch-querier startup interval: 31 secs, count: 2
 Switch-querier robustness: 2
 IGMP configured version is v3
 IGMP Operating version is v3
```

IGMP Querier information includes:

- VLAN number
- Querier status
  - Other IGMP querier—none
  - IGMP querier present, address: (IP or MAC address)
    Other IGMP querier present, interval (minutes:seconds)
- Querier election type (IPv4 or MAC) and address
- Query interval
- Querier startup interval
- Maximum query response interval
- Querier robustness value
- IGMP version number

IGMP Group Information

The following command displays IGMP Group information:

`show ip igmp groups`

Command mode: All

```
Total entries: 5  Total IGMP groups: 2
Note: The <Total IGMP groups> number is computed as
      the number of unique (Group, Vlan) entries!
Note: Local groups (224.0.0.x) are not snooped and will not appear.
Source        Group           VLAN    Port   Version  Mode  Expires Fwd
------------- --------------- ------- ------ -------- ----- ------- ---
10.1.1.1      232.1.1.1        2      4       V3       INC    4:16  Yes
10.1.1.5      232.1.1.1        2      4       V3       INC    4:16  Yes
*             232.1.1.1        2      4       V3       INC     -    No
10.10.10.43   235.0.0.1        9      1       V3       EXC    2:26  No
*             235.0.0.1        9      1       V3       EXC     -    Yes
```

IGMP Group information includes:

- IGMP source address
- IGMP Group address
- VLAN and port
- IGMP version
- IGMPv3 filter mode
- Expiration timer value
- IGMP multicast forwarding state

IGMP Multicast Router Information

The following command displays Mrouter information:

`show ip igmp mrouter information`

Command mode: All

```
Total entries: 3 Total number of dynamic mrouters: 2
Total number of installed static mrouters: 1
SrcIP               VLAN    Port    Version   Expires  MRT     QRV   QQIC
------------------- ------- ------- --------- -------- ------- ----  ----
10.1.1.1            2       21      V3        4:09     128     2     125
10.1.1.5            2       23      V2        4:09     125     -     -
*                   9       24      V2        static           -     -
```

IGMP Mrouter information includes:

- Source IP address
- VLAN and port where the Mrouter is connected
- IGMP version
- Mrouter expiration
- Maximum query response time
- Querier's Robustness Variable (QRV)
- Querier's Query Interval Code (QQIC)

IPMC Group Information

The following command displays IGMP IPMC group information:

`show ip igmp ipmcgrp`

Command mode: All

```
Total number of displayed ipmc groups: 4
Legend(possible values in Type column):
SH - static host      DR - dynamic registered
SP - static primary   DU - dynamic unregistered
SB - static backup     M - mrouter
 O - other
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
     Source          Group      Vlan    Port      Type  Timeleft
=============== =============== ==== ============ ==== ==========
       *            232.0.0.1     1      -         DU   6 sec
       *            232.0.0.2     1      -         DU   6 sec
       *            232.0.0.3     1      -         DU   6 sec
       *            232.0.0.4     1      -         DU   6 sec
```

IGMP IPMC Group information includes:

- IGMP source address
- IGMP group address
- VLAN and port
- Type of IPMC group
- Expiration timer value

MLD Information

The following table describes the commands used to view MLD information.

Table 53. *MLD Information Commands*

Command Syntax and Usage
show ipv6 mld groups Displays MLD multicast group information. **Command mode:** All
show ipv6 mld groups address *<IPv6 address>* Displays group information for the specified IPv6 address. **Command mode:** All
show ipv6 mld groups interface port *<port alias or number>* Displays MLD groups on a single interface port. **Command mode:** All
show ipv6 mld groups portchannel *<1-144>* Displays groups on a single port channel. **Command mode:** All
show ipv6 mld groups vlan *<VLAN ID (1-4094)>* Displays groups on a single VLAN. **Command mode:** All
show ipv6 mld interface [*<1-126>***]** Displays information for all MLD interfaces or a specific MLD interface. **Command mode:** All
show ipv6 mld mrouter Displays all MLD Mrouter ports. See page 122 for sample output. **Command mode:** All

MLD Mrouter Information

The following command displays MLD Mrouter information:

`show ipv6 mld mrouter`

Command mode: All

```
Source: fe80:0:0:0:200:14ff:fea8:40c9
Port/Vlan: 26/4
Interface: 3
QRV: 2  QQIC:125
Maximum Response Delay: 1000
Version: MLDv2 Expires:1:02
```

The following table describes the MLD Mrouter information displayed in the output.

Table 54. *MLD Mrouter*

Statistic	Description
Source	Displays the link-local address of the reporter.
Port/Vlan	Displays the port/vlan on which the general query is received.
Interface	Displays the interface number on which the general query is received.
QRV	Displays the Querier's robustness variable value.
QQIC	Displays the Querier's query interval code.
Maximum Response Delay	Displays the configured maximum query response time.
Version	Displays the MLD version configured on the interface.
Expires	Displays the amount of time that must pass before the multicast router decides that there are no more listeners for a multicast address or a particular source on a link.

VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on RackSwitch G8272 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

The following table describes commands to view VRRP information:

Table 55. *VRRP Information Commands*

Command Syntax and Usage
show ip vrrp Displays the current VRRP parameters. **Command mode:** All
show ip vrrp group Displays the current configuration information for the virtual router group. **Command mode:** All
show ip vrrp group track Displays the current configuration for priority tracking for the virtual router. **Command mode:** All
show ip vrrp information Displays VRRP information. For details, see page 124. **Command mode:** All
show ip vrrp interface *<1-126>* Displays the current configuration for this IP interface's authentication parameters. **Command mode:** All
show ip vrrp tracking-priority-increment Displays the current configuration of priority tracking increment values. **Command mode:** All
show ip vrrp virtual-router *<1-128>* Displays the current configuration information for this virtual router. **Command mode:** All
show ip vrrp virtual-router *<1-128>* **track** Displays the current configuration for priority tracking for this virtual router. **Command mode:** All

The following command displays VRRP information:

`show ip vrrp information`

Command mode: All

```
VRRP information:
  1: vrid 2, 205.178.18.210, if  1, renter, prio 100, master
  2: vrid 1, 205.178.18.202, if  1, renter, prio 100, backup
  3: vrid 3, 205.178.18.204, if  1, renter, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event. For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner) or transitions to backup if it is not the IP address owner.

Interface Information

The following command displays interface information:

`show interface ip`

Command mode: All

```
Interface information:
1:     IP4 192.168.49.50   255.255.255.0   192.168.49.255, vlan 1,  DOWN
2:     IP6 3003:0:0:0:0:0:5/64 ,                          vlan 2,    up
           fe80::213:aff:fe4f:7c02
128:   IP4 192.168.50.50   255.255.255.0   192.168.50.255, vlan 4095, up

Routed Port Interface Information:

Loopback interface information:
lo1: 192.168.48.48   255.255.255.128 192.168.48.127,          up
```

For each interface, the following information is displayed:

- IPv4 interface address and subnet mask
- IPv6 address and prefix
- VLAN assignment
- Status (up, down, or disabled)

IPv6 Interface Information

The following command displays IPv6 interface information:

`show ipv6 interface` *<interface number>*

Command mode: All

```
Interface information:
  2: IP6 2001:0:0:0:225:3ff:febb:bb15/64            , vlan 1, up
         fe80::225:3ff:febb:bb15
    Link local address:
        fe80::225:3ff:febb:bb15
    Global unicast address(es):
        2001::225:3ff:febb:bb15/64
    Anycast address(es):
        Not Configured.
    Joined group address(es):
        ff02::1
        ff02::2
        ff02::1:ffbb:bb15
    MTU is 1500
    ICMP redirects are enabled
    ND DAD is enabled, Number of DAD attempts: 1
    ND router advertisement is disabled
```

For each interface, the following information is displayed:

- IPv6 interface address and prefix
- VLAN assignment
- Status (up, down or disabled)
- Path MTU size
- Status of ICMP redirects
- Status of Neighbor Discovery (ND) Duplicate Address Detection (DAD)
- Status of Neighbor Discovery router advertisements

IPv6 Path MTU Information

The following command displays IPv6 Path MTU information:

`show ipv6 pmtu [`*<destination IPv6 address>***`]`**

Command mode: All

```
Path MTU Discovery info:

Max Cache Entry Number : 10
Current Cache Entry Number: 2
Cache  Timeout Interval : 10 minutes

Destination Address                       Since       PMTU
5000:1::3                                 00:02:26    1400
FE80::203:A0FF:FED6:141D                  00:06:55    1280
```

Path MTU Discovery information provides information about entries in the Path MTU cache. The PMTU field indicates the maximum packet size in octets that can successfully traverse the path from the switch to the destination node. It is equal to the minimum link MTU of all the links in the path to the destination node.

IP Information

The following command displays Layer 3 information:

`show ip interface brief`

Command mode: All

```
IP information:
  AS number 0

Interface information:
1:     IP4 192.168.49.50   255.255.255.0   192.168.49.255,  vlan 1, DOWN
128:   IP4 192.168.50.50   255.255.255.0   192.168.50.255,  vlan 4095, up

Loopback interface information:
lo1: 192.168.48.48   255.255.255.128 192.168.48.127,          up

Default gateway information: metric strict

Default IP6 gateway information:

ECMP Hash Mechanism: dipsip

Current BOOTP relay settings: OFF
Global servers:
------------------------
Server 1 address 0.0.0.0
Server 2 address 0.0.0.0
Server 3 address 0.0.0.0
Server 4 address 0.0.0.0
Server 5 address 0.0.0.0

Current BOOTP relay option-82 settings: OFF
Current BOOTP relay option-82 policy: Replace

Current DHCP Snooping settings: Off
DHCP Snooping is configured on the following VLANs: empty

Insertion of option 82 information is Disable
      Interface   Trusted    Rate limit (pps)
-------------------------------------------
              1        No                none
              2        No                none
              3        No                none
              4        No                none
              5        No                none
            ...

Current IP forwarding settings: ON, dirbr disabled, noicmprd disabled,
ICMPv6 redirect disabled
Current network filter settings: none
Current route map settings: none
RIP is disabled.
OSPF is disabled.
Current OSPFv3 settings: OSPFv3 is disabled.
Current PIM settings: OFF
BGP is disabled
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address and health status
- BootP relay settings
- IP forwarding settings, including the forwarding status of directed broadcasts and the status of ICMP re-directs
- Network filter settings, if applicable
- Route map settings, if applicable

IKEv2 Information

The following table lists commands that display information about IKEv2.

Table 56. *IKEv2 Information Commands*

Command Syntax and Usage
show ikev2 Displays all IKEv2 information. See page 131 for sample output. **Command mode:** All
show ikev2 ca-cert Displays the CA certificate. **Command mode:** All
show ikev2 host-cert Displays the host certificate. **Command mode:** All
show ikev2 identity Displays IKEv2 identity information. **Command mode:** All
show ikev2 preshare-key Displays the IKEv2 preshare key. **Command mode:** All
show ikev2 proposal Displays the IKEv2 proposal. **Command mode:** All
show ikev2 retransmit-interval Displays the IKEv2 retransmit interval. **Command mode:** All
show ikev2 sa Displays the IKEv2 SA. **Command mode:** All

IKEv2 Information Dump

The following command displays IKEv2 information:

`show ikev2`

Command mode: All

```
IKEv2 retransmit time:       20

IKEv2 cookie notification:   disable

IKEv2 authentication method: Pre-shared key

IKEv2 proposal:
Cipher:                      3des
Authentication:              sha1
DH Group:                    dh-24

Local preshare key:          ibm123

IKEv2 choose IPv6 address as ID type
```

IKEv2 information includes:

- IKEv2 retransmit time, in seconds.
- Whether IKEv2 cookie notification is enabled.
- The IKEv2 proposal in force. This includes the encryption algorithm (cipher), the authentication algorithm type and the Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. Higher DH group numbers are more secure but require additional time to compute the key.
- The local preshare key.
- Whether IKEv2 is using IPv4 or IPv6 addresses as the ID type.

IP Security Information

The following table describes the commands used to display information about IP security.

Table 57. *IPsec Information Commands*

Command Syntax and Usage
show ipsec dynamic-policy [*<1-10>***]** Displays dynamic policy information. **Command mode:** All
show ipsec manual-policy [*<1-10>***]** Displays manual policy information. See page 133 for sample output. **Command mode:** All
show ipsec sa Displays all security association information. **Command mode:** All
show ipsec spd Displays all security policy information. **Command mode:** All
show ipsec traffic-selector [*<1-10>***]** Displays IPsec traffic selector information. **Command mode:** All
show ipsec transform-set [*<1-10>***]** Displays IPsec transform set information. **Command mode:** All

IPsec Manual Policy Information

The following command displays IPsec manual key management policy information:

`show ipsec manual-policy`

Command mode: All

```
IPsec manual policy 1 --------------------------------
IP Address:                      2002:0:0:0:0:0:0:151
Associated transform ID:         1
Associated traffic selector ID:  1
IN-ESP SPI:                      9900
IN-ESP encryption KEY:           3456789abcdef012
IN-ESP authentication KEY:       23456789abcdef0123456789abcdef0123456789
OUT-ESP SPI:                     7700
OUT-ESP encryption KEY:          6789abcdef012345
OUT-ESP authentication KEY:      56789abcdef0123456789abcdef0123456789abc
Applied on interface:
interface 1
```

IPsec manual policy information includes:

- The IP address of the remote peer
- The transform set ID associated with this policy
- Traffic selector ID associated with this policy
- ESP inbound SPI
- ESP inbound encryption key
- ESP inbound authentication key
- ESP outbound SPI
- ESP outbound encryption key
- ESP outbound authentication key
- The interface to which this manual policy has been applied

DHCP Snooping Information

The following command displays DHCP Snooping information:

show ip dhcp snooping

Command mode: All

```
DHCP Snooping is configured on the following VLANs:
 empty
Insertion of option 82 information is Disable
      Interface   Trusted    Rate limit (pps)
-----------------------------------
              1        No                none
              5        No                none
              6        No                none
              7        No                none
              8        No                none
              9        No                none
             10        No                none
             11        No                none
             12        No                none
             13        No                none
             14        No                none
             15        No                none
...
```

The following command displays the DHCP binding table:

show ip dhcp snooping binding

Command mode: All

```
Mac Address        IP Address       Lease(seconds) Type     VLAN Interface
-------------------------------------------------------------------------------
00:00:01:00:02:01  10.0.0.1         1600           dynamic  100  port 1
02:1c:5f:d1:18:9c  210.38.197.63    86337          Static   127   1
06:51:4d:e6:16:2d  194.116.155.190  86337          Static   105   1
08:69:0f:1d:ba:3d  40.90.17.26      86337          Static   150   1
08:a2:6d:00:36:56  40.194.18.213    86337          Static   108   1
0e:a7:f8:a2:74:2c  130.254.47.129   86337          Static   171   1
0e:b7:64:02:97:7c  35.92.27.110     86337          Static   249   1

Total number of bindings: 7
```

The DHCP Snooping binding table displays information for each entry in the table. Each entry has a MAC address, an IP address, the lease time, the interface to which the entry applies and the VLAN to which the interface belongs.

PIM Information

The following commands display PIM information:

Table 58. *PIM Information Options*

Command Syntax and Usage
show ip pim bsr [<*component ID (1-2)*>**]** Displays information about the PIM bootstrap router (BSR). **Command mode:** All
show ip pim component [<*component ID (1-2)*>**]** Displays PIM component information. For details, see page 136. **Command mode:** All
show ip pim elected-rp [group <*multicast group IP address*>**]** Displays a list of the elected Rendezvous Points. **Command mode:** All
show ip pim interface [<*1-126*>**|detail|loopback** <*1-5*>**|port** <*port alias or number*>**]** Displays PIM interface information. To view sample output, see page 136. **Command mode:** All
show ip pim mroute Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see page 138. **Command mode:** All
show ip pim neighbor [<*interface number*>**|port** <*port alias or number*>**]** Displays PIM neighbor information. To view sample output, see page 137. **Command mode:** All
show ip pim neighbor-filters Displays information about PIM neighbor filters. **Command mode:** All
show ip pim rp-candidate [<*component ID (1-2)*>**]** Displays a list of the candidate Rendezvous Points configured. **Command mode:** All
show ip pim rp-set [<*RP IP address*>**]** Displays a list of the Rendezvous Points learned. **Command mode:** All
show ip pim rp-static [<*component ID (1-2)*>**]** Displays a list of the static Rendezvous Points configured. **Command mode:** All

PIM Component Information

The following command displays Protocol Independent Multicast (PIM) component information:

`show ip pim component [`<*component ID (1-2)*>**`]`**

Command mode: All

```
PIM Component Information
-------------------------
Component-Id: 1
  PIM Mode: sparse,   PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0
```

PIM component information includes the following:

- Component ID
- Mode (sparse, dense)
- PIM Version
- Elected Bootstrap Router (BSR) address
- Candidate Rendezvous Point (RP) hold time, in seconds

PIM Interface Information

The following command displays information about PIM interfaces:

`show ip pim interface`

Command mode: All

```
Address  IfName/IfId Ver/Mode Nbr Qry DR-Address DR-Prio Count Interval
-------- ---------- -------- --- --- ---------- ------- --------------
40.0.0.3 net4/4      2/Sparse 1   30  40.0.0.3           1
50.0.0.3 net5/5      2/Sparse 0   30  50.0.0.3           1
```

PIM interface information includes the following for each PIM interface:

- IP address
- Name and ID
- Version and mode
- Neighbor count
- Query interval
- Designated Router address
- Designated Router priority value

PIM Neighbor Information

The following command displays PIM neighbor information:

`show ip pim neighbor`

Command mode: All

```
Neighbour IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override Lan
Address                                                  Interval Delay
--------- ---------- ------------ --- ---------- ------ -------- -----
40.0.0.2  net4/4     00:00:37/79    v2     1/S         1        0     0
40.0.0.4  net1/160   00:03:41/92    v2    32/S         2        0     0
```

PIM neighbor information includes the following:

- Neighbor IP address, interface name and interface ID
- Name and ID of interface used to reach the PIM neighbor
- Up time (the time since this neighbor became the neighbor of the local router)
- Expiry Time (the minimum time remaining before this PIM neighbor expires)
- Version number
- Designated Router priority and mode
- Component ID
- Override interval
- LAN delay interval

PIM Multicast Route Information Commands

The following commands display PIM Multicast Route information:

Table 59. *PIM Multicast Route Information Options*

Command Syntax and Usage
show ip pim mroute Displays information about all PIM multicast routes. **Command mode:** All
show ip pim mroute [<*component ID (1-2)*>**]** Displays PIM multicast routes for the selected component. **Command mode:** All
show ip pim mroute count Displays a count of PIM multicast routes of each type. **Command mode:** All
show ip pim mroute flags [s] [r] [w] Displays PIM multicast routes based on the selected entry flags. Enter flags in any combination: o **s**: Shortest Path Tree (SPT) bit o **r**: Rendezvous Point Tree (RPT) bit o **w**: Wildcard bit **Command mode:** All
show ip pim mroute group <*multicast group IP address*> Displays PIM multicast routes for the selected multicast group. **Command mode:** All
show ip pim mroute interface {<*interface number*>**|port** <*port alias or number*>**}** Displays PIM multicast routes for the selected incoming IP interface. **Command mode:** All
show ip pim mroute source <*multicast source IP address*> Displays PIM multicast routes for the selected source IP address. **Command mode:** All

PIM Multicast Route Information

The following command displays PIM multicast route information:

`show ip pim mroute`

Command mode: All

```
IP Multicast Routing Table
--------------------------
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires

(8.8.8.111, 224.2.2.100) ,00:42:03/00:01:11
 Incoming Interface : net44 ,RPF nbr : 44.44.44.1 ,Route Flags : S
  Outgoing InterfaceList :
    net17, Forwarding/Sparse ,00:42:03/---

(*, 224.2.2.100) ,00:45:15/--- ,RP : 88.88.88.2
 Incoming Interface : net5 ,RPF nbr : 5.5.5.2 ,Route Flags : WR
  Outgoing InterfaceList :
    net17, Forwarding/Sparse ,00:45:15/---

Total number of (*,G) entries : 1
Total number of (S,G) entries : 1
```

Quality of Service Information

The following commands display QoS information:

Table 60. *QoS information Options*

Command Syntax and Usage
show qos protocol-packet-control information queue [all] Displays the packet rate configured for each configurable packet queue. The `all` option also displays the packet rate configured for each reserved packet queue. **Command mode:** All
show qos protocol-packet-control information protocol Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. **Command mode:** All
show qos random-detect Displays WRED and ECN information. For details, see page 142. **Command mode:** All
show qos transmit-queue Displays the current 802.1p parameters. **Command mode:** All
show qos transmit-queue information Displays all 802.1p information. For details, see page 141. **Command mode:** All

802.1p Information

The following command displays 802.1p information:

`show qos transmit-queue information`

Command mode: All

```
Current priority to COS queue information:
Priority  COSq  Weight
--------  ----  ------
    0       0      1
    1       1      2
    2       2      3
    3       3      4
    4       4      5
    5       5      7
    6       6     15
    7       7      0

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
1           0       0      1
2           0       0      1
3           0       0      1
4           0       0      1
5           0       0      1
6           0       0      1
7           0       0      1
8           0       0      1
9           0       0      1
10          0       0      1
...
50          0       0      1
51          0       0      1
52          0       0      1
53          0       0      1
54          0       0      1
MGT         0       0      1
```

The following table describes the IEEE 802.1p priority-to-COS queue information.

Table 61. *802.1p Priority-to-COS Queue Parameter Descriptions*

Parameter	Description
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight of the COS queue.

The following table describes the IEEE 802.1p port priority information.

Table 62. *802.1p Port Priority Parameter Descriptions*

Parameter	Description
Port	Displays the port alias.
Priority	Displays the 802.1p Priority level.
COSq	Displays the Class of Service queue.
Weight	Displays the scheduling weight.

WRED and ECN Information

The following command displays WRED and ECN information:

`show qos random-detect`

Command mode: All

```
Current wred and ecn configuration:
Global ECN:  Disable
Global WRED: Disable

    --WRED--TcpMinThr--TcpMaxThr--TcpDrate--NonTcpMinThr--NonTcpMaxThr--NonTcpDrate--
TQ0:  Dis       0          0          0          0             0             0
TQ1:  Dis       0          0          0          0             0             0
TQ2:  Dis       0          0          0          0             0             0
TQ3:  Dis       0          0          0          0             0             0
TQ4:  Dis       0          0          0          0             0             0
TQ5:  Dis       0          0          0          0             0             0
TQ6:  Dis       0          0          0          0             0             0
TQ7:  Dis       0          0          0          0             0             0
```

Access Control List Information

The following commands display Access Control List (ACL) information:

Table 63. *ACL Information Options*

Command Syntax and Usage
show access-control group [*<1-256>***]** Displays ACL group information. **Command mode:** All
show access-control list [*<1-256>***]** Displays ACL list information. For details, see page 144. **Command mode:** All
show access-control list6 [*<1-128>***]** Displays IPv6 ACL list information. For details, see page 146. **Command mode:** All
show access-control log Displays the current ACL log parameters. **Command mode:** All
show access-control macl [*<1-256>***]** Displays the current MACL parameters. **Command mode:** All
show access-control vmap [*<1-128>***]** Displays VMAP information. **Command mode:** All

Access Control List Information

The following commands display IPv4 Access Control List (ACL) information:

Table 64. *IPv4 Access Control List Information Commands*

Command Syntax and Usage
show access-control list [<*1-256*>**]** Displays ACL list information. To view sample output, see page 145. **Command mode:** All
show access-control list <*1-256*> **ethernet** Displays the current Ethernet parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **ipv4** Displays the current IPv4 parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **log** Displays the current IPv4 ACL log state. **Command mode:** All
show access-control list <*1-256*> **meter** Displays the current metering parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **mirror** Displays the current port mirroring parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **packet-format** Displays the current Packet Format parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **re-mark** Displays the current re-mark parameters for the specified ACL. **Command mode:** All
show access-control list <*1-256*> **tcp-udp** Displays the current TCP/UDP Filtering parameters for the specified ACL. **Command mode:** All

The following command displays Access Control List (ACL) information:

`show access-control list` *<1-256>*

Command mode: All

```
Current ACL List information:
-----------------------
Filter 1 profile:
   Ethernet
     - SMAC       : 00:00:aa:aa:01:fe/ff:ff:ff:ff:ff:ff
     - DMAC       : 00:0d:60:9c:ec:d5/ff:ff:ff:ff:ff:ff
     - VID        : 10/0xfff
     - Ethertype  : IP (0x0800)
     - Priority   : 3
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Packet Format
     - Ethernet format : None
     - Tagging format  : Any
     - IP format       : None
   Actions        : Deny
   Statistics     : enabled

Mirror Target Configuration:
        Mirror target destination: port
        Egress port for mirror target: 4
```

If the ACL is being used with Policy-Based Routing (PBR), the output from this command is more like the following:

```
Filter 1 profile: route-map 16
   IPv4
     - Protocol   : 17
   Actions        : Permit
                  : dscp 22
   Statistics     : enabled
   Installed on Port 16
```

Access Control List (ACL) information includes configuration settings for each ACL.

Table 65. *ACL List Parameter Descriptions*

Parameter	Description
Filter x profile	Indicates the ACL number.
Ethernet	Displays the ACL Ethernet header parameters, if configured.
IPv4	Displays the ACL IPv4 header parameters, if configured.
TCP/UDP	Displays the ACL TCP/UDP header parameters, if configured.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.

Table 65. *ACL List Parameter Descriptions*

Parameter	Description
Packet Format	Displays the ACL Packet Format parameters, if configured.
Actions	Displays the configured action for the ACL.
Statistics	Displays status of ACL statistics (enabled or disabled).
Mirror Target Configuration	Displays ACL port mirroring parameters.
Filter x profile	Indicates the ACL number.

Access Control IPv6 List Information

The following commands display IPv6 Access Control List (ACL) information:

Table 66. *IPv6 Access Control List Information Commands*

Command Syntax and Usage
show access-control list6 [<*1-128*>**]** Displays the current ACL parameters. **Command mode:** All
show access-control list6 <*1-128*> **ipv6** Displays the current IPv6 parameters for the specified ACL. **Command mode:** All
show access-control list6 <*1-128*> **log** Displays the current IPv6 ACL log state. **Command mode:** All
show access-control list6 <*1-128*> **meter** Displays current metering parameters for the specified ACL. **Command mode:** All
show access-control list6 <*1-128*> **re-mark** Displays current re-mark parameters for the specified ACL. **Command mode:** All
show access-control list6 <*1-128*> **tcp-udp** Displays the current TCP/UDP Filtering parameters for the specified ACL. **Command mode:** All

NAT Information

The following commands display information about Network Address Translation (NAT) settings.

Table 67. *NAT Information Options*

Command Syntax and Usage
`show ip nat` Displays NAT status information. **Command mode:** Privileged EXEC
`show ip nat translations` Displays configured translation entries list. For more information, see page page 148. **Command mode:** Privileged EXEC
`show ip nat translations full` Displays configured translation entries list with counters for both directions. For more information, see page page 148. **Command mode:** Privileged EXEC

NAT Status Information

The following command displays current NAT information:

`show ip nat`

Command mode: Privileged EXEC

```
Network address translation status: ENABLED.
Dynamic timeout expiry time is 300 seconds.
There are 5 entries in the NAT table, out of which
  3 installed in hardware table
  1 not installed because of missing egress
  0 dynamically learned entries
  5 statically configured entries
  0 software only entries
There are 0 configured dynamic rules.
Following vlans are configured as inside: 1
Following vlans are configured as outside: 2
```

NAT Translations Information

The following command displays configured NAT translations entries list:

`show ip nat translations`

Command mode: Privileged EXEC

```
Pro Inside global   Inside local   Outside local  Outside global Flags
any ---             ---            51.1.2.1       102.1.2.1      OI
any 95.1.1.1        149.1.1.1      ---            ---            ID
any ---             ---            95.4.1.1       95.3.1.1
any ---             ---            51.3.1.1       104.1.1.1       I
tcp 172.9.9.142:777 12.2.2.42:444  ---            ---
tcp ---             ---            23.1.1.133:333 210.3.3.33:555
udp 96.1.1.1:80     149.2.1.1:1080 ---            ---

Flags: O-one way, I-installed, D-dynamic
```

Use the following command to display also counters for both directions:

`show ip nat translations full`

Command mode: Privileged EXEC

```
                    inside-outside
Pro Inside global   Inside local   packet count
any ---             ---            0x6
any 95.1.1.1        149.1.1.1      0x8
any ---             ---            0x0
any ---             ---            0x131
tcp 172.9.9.142:777 12.2.2.42:444  0x0
tcp ---             ---            0x0
udp 96.1.1.1:80     149.2.1.1:1080 0x0

                    outside-inside
Outside local  Outside global packet count Flags
51.1.2.1       102.1.2.1      0x0          OI
---            ---            0x9          ID
95.4.1.1       95.3.1.1       0x0
51.3.1.1       104.1.1.1      0x0          I
---            ---            0x0
23.1.1.133:333 210.3.3.33:555 0x0
---            ---            0x0

Flags: O-one way, I-installed, D-dynamic
```

OpenFlow Information

The following commands display OpenFlow information.

Table 68. *OpenFlow Information Options*

Command Syntax and Usage
`show openflow [flow-allocation|group|information|table]` Displays the current OpenFlow configuration. For more information, see page 150. o `flow-allocation` displays the configured, current and maximum number of flows for all OpenFlow instances. For more information, see page 152. o `group` displays group information for all OpenFlow 1.3 instances. For more information, see page 154. o `information` displays the configuration for all OpenFlow instances. For more information, see page 155. o `table` displays the basic and emergency flow tables for all OpenFlow instances. For more information, see page 157. **Command mode**: All
`show openflow instance` *<1-2>* **`[group|information|table]`** Displays OpenFlow information for the specified instance ID: o `group` displays group information per instance o `information` displays the instance configuration o `table` displays the basic and emergency flow tables per instance **Command mode:** All

OpenFlow Global Configuration Information

The following command displays the global OpenFlow configuration parameters for all instances:

`show openflow`

Command mode: All

In OpenFlow 1.0:

```
Protocol Version: 1.0
Openflow State: Enabled
FDB Table Priority: 1000
FDB Table FDB-timeout: Disabled

Openflow Instance ID: 1
    state: disabled , buffering: disabled
    retry 4, emergency time-out 30
    echo req interval 30, echo reply time-out 15
    min-flow-timeout : use controller provided values.
    max flows acl           : Maximum Available
    max flows unicast fdb   : Maximum Available
    max flows multicast fdb : Maximum Available
    emergency feature: disabled
    dpid: 0x0001a897dcf7e600


Openflow Instance ID: 2
    state: enabled , buffering: disabled
    retry 4, emergency time-out 30
    echo req interval 30, echo reply time-out 15
    min-flow-timeout : use controller provided values.
    max flows acl           : Maximum Available
    max flows unicast fdb   : Maximum Available
    max flows multicast fdb : Maximum Available
    emergency feature: disabled
    dpid: 0x0002a897dcf7e600
```

In OpenFlow 1.3:

```
Protocol Version: 1.3.1
Openflow State: Enabled
FDB Table Priority: 1000
MPLS Table Priority: 65535
FDB Table FDB-timeout: Disabled

Openflow Instance ID: 1
    state: enabled , buffering: disabled , table-miss: drop
    echo req interval 30, echo reply time-out 15, retry 4
    min-flow-timeout : use controller provided values.
    max flows acl           : Maximum Available
    max flows unicast fdb   : Maximum Available
    max flows multicast fdb : Maximum Available
    max flows mpls push : Maximum Available
    max flows mpls pop : Maximum Available
    dpid: 0x0001a897dcf7e600
    table-miss cookie: 0xffffffffffffffff
    mirror-to-controller cookie: 0xffffffffffffffff
    send-to-controller cookie: 0xffffffffffffffff


Openflow Instance ID: 2
    state: enabled , buffering: disabled , table-miss: drop
    echo req interval 30, echo reply time-out 15, retry 4
    min-flow-timeout : use controller provided values.
    max flows acl           : Maximum Available
    max flows unicast fdb   : Maximum Available
    max flows multicast fdb : Maximum Available
    max flows mpls push : Maximum Available
    max flows mpls pop : Maximum Available
    dpid: 0x0002a897dcf7e600
    table-miss cookie: 0xffffffffffffffff
    mirror-to-controller cookie: 0xffffffffffffffff
    send-to-controller cookie: 0xffffffffffffffff
```

OpenFlow Flow Allocation Information

The following command displays the OpenFlow flow allocation for all instances:

`show openflow flow-allocation`

Command mode: All

In OpenFlow 1.0:

```
Flow Allocation Information


Instance 1

Maximum ACL Count Configured          : Maximum Available
Maximum Unicast FDB Count Configured  : Maximum Available
Maximum Multicast FDB Count Configured: Maximum Available

Basic Entries

Current ACL Count                     : 0
Current Unicast FDB Count             : 0
Current Multicast FDB Count           : 0

Emergency Entries

Current ACL Count                     : 0
Current Unicast FDB Count             : 0
Current Multicast FDB Count           : 0

Maximum Current Availability

Maximum Available ACL Count          : 1500
Maximum Available Unicast FDB Count  : 123904
Maximum Available Multicast FDB Count: 4096

Instance 2
...
```

In OpenFlow 1.3:

```
Flow Allocation Information


Instance 1

Maximum ACL Count Configured          : Maximum Available
Maximum Unicast FDB Count Configured  : Maximum Available
Maximum Multicast FDB Count Configured: Maximum Available
Maximum MPLS PUSH Count Configured    : Maximum Available
Maximum MPLS POP Count Configured     : Maximum Available

Basic Entries

Current ACL Count                     : 0
Current Unicast FDB Count             : 0
Current Multicast FDB Count           : 0
Current MPLS PUSH Count               : 0
Current MPLS POP Count                : 0

Static Entries

Current static ACL Count              : 0
Current static MPLS PUSH Count        : 0
Current static MPLS POP Count         : 0

Maximum Current Availability

Maximum Available ACL Count           : 1500
Maximum Available Unicast FDB Count   : 123904
Maximum Available Multicast FDB Count : 4096
Maximum Available MPLS PUSH Count     : 2000
Maximum Available MPLS POP Count      : 1000

Instance 2
...
```

OpenFlow Group Information

The following command displays the OpenFlow 1.3 group information for all instances:

show openflow group

Command mode: All

```
Openflow Instance Id: 1

Group count: 3

Group 1, Type: ALL, Bucket count: 2
  Bucket #0: output:INGRESS
  Bucket #1: output:1
Group 2, Type: ALL, Bucket count: 2
  Bucket #0: output:INGRESS
  Bucket #1: output:PCH64
Group 3, Type: ALL, Bucket count: 2
  Bucket #0: output:PCH52
  Bucket #1: output:PCH64
Openflow instance 2 is currently disabled
```

OpenFlow Configuration Information

The following command displays the OpenFlow configuration for all instances:

`show openflow information`

Command mode: All

In OpenFlow 1.0:

```
Openflow feature is Enabled
------------------------------------------------------------

Openflow instance 1 is currently disabled
------------------------------------------------------------
Openflow Instance ID: 2
        State : Enabled
        DataPath ID: 0x0002749975ab5c00
        Max Retries per controller: 4
        Echo Request Interval: 30
        Echo Reply Timeout: 15
        Emergency Timeout: 30
        Min-flow-timeout : 0, use controller provided values.
        Max ACL Flows: Maximum Available
        Max Unicast FDB Flows: Maximum Available
        Max Multicast FDB Flows: Maximum Available
        Buffering: Disabled
        Operational Mode: Normal
        Miss Send Len: 65535

Port  Alias  Status  State  Config  Current  Advertised  Supported  Peer
18    18       e     0x200  0x2     0xc0     0x0         0x0        0x0
19    19       e     0x200  0x2     0xc0     0x0         0x0        0x0
24    24       d     0x201  0x2     0xc0     0x0         0x0        0x0

Number of Ports: 7
Configured Controllers:
        Openflow Controller 1:
                IP Address: 9.70.31.71
                Port: 6633
                State: Active
                Retry Count: 0
```

In OpenFlow 1.3:

```
Openflow feature is Enabled
------------------------------------------------------------
Openflow Instance ID: 1
        State : Enabled
        DataPath ID: 0x000000000000ac01
        Table-miss cookie: 0xffffffffffffffff
        Mirror-to-controller cookie: 0xffffffffffffffff
        Send-to-controller cookie: 0xffffffffffffffff
        Max Retries per controller: 4
        Echo Request Interval: 30
        Echo Reply Timeout: 15
        Min-flow-timeout : 0, use controller provided values.
        Max ACL Flows: Maximum Available
        Max Unicast FDB Flows: Maximum Available
        Max Multicast FDB Flows: Maximum Available
        Max MPLS Push Flows: Maximum Available
        Max MPLS Pop Flows: Maximum Available
        Buffering: Disabled
        Table Miss: Drop
        Operational Mode: Normal
        Miss Send Len: 65535

Port  Alias  Status  State  Config  Current  Advertised  Supported  Peer
18    18        e     0x0    0x0     0x840      0x0        0x0      0x0
64    64        e     0x0    0x0     0x2820     0x0        0x0      0x0
10065 PCH65     e     0x0    0x0     0xc00      0x0        0x0      0x0
10066 PCH66     e     0x0    0x0     0xc00      0x0        0x0      0x0

Number of Ports: 2
Number of Portchannels: 2

Configured Controllers:
        Openflow Controller 1:
                IP Address: 9.228.143.62
                Port: 6633
                State: Active

------------------------------------------------------------

Openflow instance 2 is currently disabled
```

OpenFlow Table Information

The following command displays the basic and emergency flow tables for all instances:

`show openflow table`

Command mode: All

In OpenFlow 1.0:

```
Openflow instance 1 is currently disabled

Openflow Instance Id: 2

BASIC FLOW TABLE

STATIC FLOWS

Flow:1 Index:1
  Filter Based, priority:  200
  QUALIFIERS:
  ACTION:  drop
  STATS:   packets=0, bytes=0

Flow:2 Index:2
  Filter Based, priority:  300
  QUALIFIERS: vlan-id: 3000
  ACTION:  Strip 802.1q Header
  STATS:   packets=0, bytes=0

Flow:3 Index:3
  Filter Based, priority: 3400
  QUALIFIERS:
  ACTION:  drop
  STATS:   packets=0, bytes=0
```

In OpenFlow 1.3:

```
Openflow instance 1 is currently disabled

Openflow Instance Id: 2

STATIC FLOWs

Flow 1, Index:1, Filter Based, priority:200
  QUALIFIERS:
  Instruction: apply_action
  ACTION:  drop
  STATS:   packets=0, bytes=0
```

OpenFlow table information includes detailed configuration information for each entry in the flow table.

Note: Flow qualifiers used for matching packets are not listed in the display if the qualifier is set to any.

RMON Information Commands

The following table describes the Remote Monitoring (RMON) Information commands.

Table 69. *RMON Information Options*

Command Syntax and Usage
show rmon Displays all RMON information. **Command mode:** All
show rmon alarm [*<1-65535>***]** Displays RMON Alarm information. For details, see page 161. **Command mode:** All
show rmon event [*<1-65535>***]** Displays RMON Event information. For details, see page 162. **Command mode:** All
show rmon history [*<1-65535>***]** Displays RMON History information. For details, see page 160. **Command mode:** All

RMON History Information

The following command displays RMON History information:

`show rmon history`

Command mode: All

```
RMON History group configuration:

Index IFOID                          Interval Rbnum Gbnum
----- ------------------------------ -------- ----- -----
   1  1.3.6.1.2.1.2.2.1.1.24               30     5     5
   2  1.3.6.1.2.1.2.2.1.1.22               30     5     5
   3  1.3.6.1.2.1.2.2.1.1.20               30     5     5
   4  1.3.6.1.2.1.2.2.1.1.19               30     5     5
   5  1.3.6.1.2.1.2.2.1.1.24             1800     5     5

Index                       Owner
-----  -------------------------------------------
    1  dan
```

The following table describes the RMON History Information parameters.

Table 70. *RMON History Parameter Descriptions*

Parameter	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.
Interval	Displays the time interval for each sampling bucket.
Rbnum	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Gbnum	Displays the number of granted buckets that may hold sampled data.
Owner	Displays the owner of the history instance.

RMON Alarm Information

The following command displays RMON alarm information:

`show rmon alarm`

Command mode: All

```
RMON Alarm group configuration:

Index  Interval  Sample   Type      rLimit       fLimit     last value
-----  --------  ------  -------  -----------  -----------  ----------
    1      1800     abs   either            0            0       7822

Index  rEvtIdx  fEvtIdx                    OID
-----  -------  -------  ----------------------------------------
    1        0        0  1.3.6.1.2.1.2.2.1.10.1

Index                       Owner
-----  ------------------------------------------
    1  dan
```

The following table describes the RMON Alarm Information parameters.

Table 71. *RMON Alarm Parameter Descriptions*

Parameter	Description
Index	Displays the index number that identifies each alarm instance.
Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Sample	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: o `abs` — absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. o `delta` — delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Type	Displays the type of alarm, as follows: o `falling` — alarm is triggered when a falling threshold is crossed. o `rising` — alarm is triggered when a rising threshold is crossed. o `either` — alarm is triggered when either a rising or falling threshold is crossed.
rLimit	Displays the rising threshold for the sampled statistic.
fLimit	Displays the falling threshold for the sampled statistic.
Last value	Displays the last sampled value.

Table 71. *RMON Alarm Parameter Descriptions (continued)*

Parameter	Description
rEvtIdx	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
fEvtIdx	Displays the falling alarm event index that is triggered when a falling threshold is crossed.
OID	Displays the MIB Object Identifier for each alarm index.
Owner	Displays the owner of the alarm instance.

RMON Event Information

The following command displays RMON event information:

`show rmon event`

Command mode: All

```
RMON Event group configuration:

Index Type    Last Sent              Description
----- ---- ---------------- --------------------------------
   1  both   0D: 0H: 1M:20S  Event_1
   2  none   0D: 0H: 0M: 0S  Event_2
   3  log    0D: 0H: 0M: 0S  Event_3
   4  trap   0D: 0H: 0M: 0S  Event_4
   5  both   0D: 0H: 0M: 0S  Log and trap event for Link Down
  10  both   0D: 0H: 0M: 0S  Log and trap event for Link Up
  11  both   0D: 0H: 0M: 0S  Send log and trap for icmpInMsg
  15  both   0D: 0H: 0M: 0S  Send log and trap for icmpInEchos

Index                       Owner
-----  ------------------------------------------
    1  dan
```

The following table describes the RMON Event Information parameters.

Table 72. *RMON Event Parameter Descriptions*

Parameter	Description
Index	Displays the index number that identifies each event instance.
Type	Displays the type of notification provided for this event, as follows: `none`, `log`, `trap` or `both`.
Last sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.
Owner	Displays the owner of the alarm instance.

Link Status Information

The following command displays link information:

`show interface status [`*<port alias or number>***`]`**

Command mode: All

```
Port     Speed    Duplex     Flow Ctrl      Link     Description
-------  -----   --------  --TX-----RX--   ------   -------------
1        1G/10G    full      no     no      down      1
2        1G/10G    full      no     no      down      2
3        1G/10G    full      no     no       up       3
4        1G/10G    full      no     no       up       4
5        1G/10G    full      no     no       up       5
6        1G/10G    full      no     no      down      6
7        1G/10G    full      no     no      down      7
8        1G/10G    full      no     no       up       8
9        1G/10G    full      no     no       up       9
10       1G/10G    full      no     no      down      10
...
51       40000     full      no     no      down      51
52       40000     full      no     no      down      52
53       40000     full      no     no      down      53
54       40000     full      no     no      down      54
MGT       1000     full     yes    yes       up       MGT
```

Use this command to display link status information about each port on the G8272, including:

- Port alias or port number
- Port description
- Port speed and Duplex mode (half, full or any)
- Flow control for transmit and receive (no, yes or both)
- Link status (up, down or disabled)

Port Information

The following command displays port information:

`show interface trunk` *<port alias or number>*

Command mode: All

```
Port    Tag RMON Lrn Fld Openflow PVID     DESCRIPTION  VLAN(s)
        Trk                       NVLAN
------- --- ---- --- --- -------- ------ -------------- -----------------
1        n   d    e   e      d       1                   1
2        n   d    e   e      d       1                   1
3        n   d    e   e      d       1                   1
4        n   d    e   e      d       1                   1
5        n   d    e   e      d       1                   1
6        n   d    e   e      d    4094                   4094
7        n   d    e   e      d       1                   1
8        n   d    e   e      d       1                   1
9        n   d    e   e      d       1                   1
10       n   d    e   e      d       1                   1
...
51       n   d    e   e      d       1                   1
52       n   d    e   e      d       1                   1
53       n   d    e   e      d       1                   1
54       n   d    e   e      d       1                   1
MGT      n   d    e   e      d    4095                   4095

* = PVID/Native-VLAN is tagged.
# = PVID is ingress tagged.
Trk  = Trunk mode
NVLAN = Native-VLAN
```

Port information includes:

- Port alias or number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB learning enabled (`Lrn`)
- Whether the port has Port Flooding enabled (`Fld`)
- Whether the port has OpenFlow enabled (Openflow)
- Whether the port uses ingress VLAN tagging or not (#)
- Whether the port uses PVID/Native-VLAN tagging or not (*)
- Port VLAN ID (`PVID`)
- Port description
- VLAN membership

Port Transceiver Status

The following command displays the status of the transceiver module on each port:

`show interface transceiver`

Command mode: All

```
Port         Link  Transceiver    Vendor         Part            Approve
------------ ----- -------------- -------------- --------------- --------
SFP+  1      LINK  SR_SFP+ 850nm  BLADE NETWORK  BN-CKM-SP-SR    Approved
SFP+  2      LINK  SX_SFP  850nm  Blade Network  BN-CKM-S-SX     Approved
SFP+  3          < NO Device Installed >
SFP+  4          < NO Device Installed >
SFP+  5          < NO Device Installed >
SFP+  6          < NO Device Installed >
SFP+  7          < NO Device Installed >
SFP+  8          < NO Device Installed >
SFP+  9          < NO Device Installed >
SFP+ 10          < NO Device Installed >
...
SFP+ 45          < NO Device Installed >
SFP+ 46          < NO Device Installed >
SFP+ 47          < NO Device Installed >
SFP+ 48          < NO Device Installed >
QSFP+  49        < NO Device Installed >
QSFP+  50        < NO Device Installed >
QSFP+  51        < NO Device Installed >
QSFP+  52        < NO Device Installed >
QSFP+  53        < NO Device Installed >
QSFP+  54        < NO Device Installed >
```

This command displays information about the transceiver module on each port, as follows:

- Port number and alias
- Link status
- Media/Transceiver type (LX, LR, SX, SR, DAC, PasDAC) and laser wavelength, in nanometers
- Vendor name
- Part number
- Approval status

Use the following command to display extended transceiver information:

`show interface port` *<port alias or number>* **`transceiver details`**

Command mode: All

```
Port             TX  Link  TXFlt Volts DegsC TXuW  RXuW  Transceiver    Approve
---------------- --- ----- ----- ----- ----- ----- ----- -------------- --------
SFP+   10        Ena LINK  -N/A- -N/A- -N/A- -N/A- -N/A- PasQD 1.0m     Approved
         BLADE NETWORK    Part:BN-QS-QS-CBL-1M  Date:110925 S/N:3548Y350VT19P8EM
```

VM Ready Information Commands

The following command display information about the VMReady feature.

Table 73. *VMReady Information Options*

Command Syntax and Usage
show virt Displays the current virtualization parameters. For a sample output, see page 169. **Command mode:** All
show virt oui Displays all the configured MAC OUIs. For a sample output, see page 169. **Command mode:** All
show virt port *<port alias or number>* Displays Virtual Machine information for the selected port. For a sample output, see page 170. **Note:** The selected port must be a server port. **Command mode:** All
show virt portchannel *<1-144>* Displays Virtual Machine information for the selected portchannel. For a sample output, see page 170. **Command mode:** All
show virt vm [-v [-r]] Displays all Virtual Machine information. o `-v` displays verbose information o `-r` rescans data center For more details, see page 171. **Command mode:** All
show virt vmcheck Displays the current VM Check settings. For a sample output, see page 171. **Command mode:** All
show virt vmgroup [*<1-4096>***]** Displays the current VM Group parameters. For a sample output, see page 172. **Command mode:** All

Table 73. *VMReady Information Options*

Command Syntax and Usage
show virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**| |**<*IP address*>**|**<*index number*>**|**<*index range*>**] [|{include|exclude| |section|begin}]** Displays the current VM bandwidth management parameters for all virtual machines or only for a certain virtual machine by specifying its MAC address, UUID, name, IP address or index number. o | displays the VM bandwidth management parameters matching one of the following filters: • `include` displays parameters matching the specified expression • `exclude` displays parameters not matching the specified expression • `section` displays parameters matching the specified section • `begin` displays parameters beginning from the first parameter that matches the specified expression For a sample output, see page 172. **Command mode:** All
show virt vmprofile [<*profile name*>**]** Displays the current VM Profile parameters. For a sample output, see page 172. **Command mode:** All
show virt vmware Displays the current VMware parameters. To view command options, see page 173. **Command mode:** All

VMReady Information

The following command displays the current virtualization options:

`show virt`

Command mode: All

```
VMready is currently enabled

Current Hello setting: disabled

Current VMware-specific settings
--------------------------------

ESX/ESXi-to-vCenter heartbeat UDP port number: 902

Current VM profiles:
--------------------
        None


VM group 1 current configuration:Current VM group's secure mode: Disabled
Current Group Ports:  13 17
Current Group vPorts: : empty
VLAN: 2
VLAN Tagging: Disabled
Current GROUP VMAP Config is empty


VM group 2 current configuration: empty
...
```

VM OUI Information

The following command displays all the configured MAC OUIs:

`show virt oui`

Command mode: All

```
        VM MAC OUI      Vendor Name
        ----------      -----------
         00:50:56       VMware
         00:0c:29       VMware
         00:05:69       VMware
         00:0f:4b       VirtualIron
         00:03:ff       Microsoft
         00:15:5d       Microsoft
         00:1c:42       Parallels
         00:16:3e       Xen
         00:80:27       Sun

        Number of MAC OUI entries: 9
```

VM Port Information

The following command displays VM information for a specific port:

show virt port *<port alias or number>*

Command mode: All

```
IP Address      VMAC Address        Index  Port  VM Group  (Profile)  Check status
--------------  ------------------  -----  ----  --------  ---------  ------------
3.3.3.2         00:50:56:a5:32:f7   0      23
40.40.31.1      00:50:56:a5:4e:9f   1      23    30        test30

Number of entries: 2
```

VM Portchannel Information

The following command displays VM information for a specific portchannel:

show virt portchannel *<1-144>*

Command mode: All

```
IP Address      VMAC Address        Index  Port  VM Group  (Profile)  Check status
--------------  ------------------  -----  ----  --------  ---------  ------------
5.5.5.2         00:50:56:a5:17:07   2      ST 5
0.0.0.0         00:50:56:a5:4b:03   4      ST 5
5.5.5.3         00:50:56:af:20:6f   3      ST 5

Number of entries: 3
0.0.0.0 indicates IP address not yet available
ST: Server Trunk
```

VM Information

The following command displays VM information:

`show virt vm`

Command mode: All

```
IP Address    VMAC Address      Index Port VM Group(Profile) Check Status
------------ ----------------- ----- ---- ----------------- ------------
*127.31.46.50 00:50:56:4e:62:f5     4    3
*127.31.46.10 00:50:56:4f:f2:85     2    4
+127.31.46.51 00:50:56:72:ec:86     1    3
+127.31.46.11 00:50:56:7c:1c:ca     3    4
 127.31.46.25 00:50:56:9c:00:c8     5    4
 127.31.46.15 00:50:56:9c:21:2f     0    4
 127.31.46.35 00:50:56:9c:29:29     6    3

Number of entries: 7
* indicates VMware ESX Service Console Interface
+ indicates VMware ESX/ESXi VMKernel or Management Interface
```

VM information includes the following for each Virtual Machine (VM):

- State of the Virtual Machine (~ indicates the VM is inactive/idle)
- IP address
- MAC address
- Index number assigned to the VM
- Server port on which the VM was detected
- VM group that contains the VM, if applicable
- VM Check status for the corresponding VM

VM Check Information

The following command displays VM Check information:

`show virt vmcheck`

Command mode: All

```
Action to take for spoofed VMs:
        Basic: Oper disable the link
        Advanced: Install ACL to drop traffic

Maximum number of acls that can be used for mac spoofing: 50
Trusted ports by configuration:  empty
```

VM Group Information

The following command displays VM Group parameters:

show virt vmgroup [*<1-4096>***]**

Command mode: All

```
VM group 1 current configuration:
Current VM group's secure mode: Disabled
Current Group Ports:  13 17
Current Group vPorts: : empty
VLAN: 2
Tagging/Trunk-mode: Disabled
Current GROUP VMAP Config is empty
```

VM Bandwidth Information

The following command displays VM bandwidth management parameters:

show virt vmpolicy vmbwidth

Command mode: All

```
Bandwidth Profile for VM 00:50:56:a5:32:f7 is enabled.
-----------------------------------------------
  TX:
    Rate:                1024
    Burst:               2048
    ACL:                  127
```

VM Profile Information

The following command displays VM Profile parameters:

show virt vmprofile

Command mode: All

```
VM profile "test30":
        VLAN ID: 30
        Traffic shaping not enabled.
        VM Groups: 30
```

VMware Information

Use these commands to display information about Virtual Machines (VMs) and VMware hosts in the data center. These commands require the presence of a configured Virtual Center.

Table 74. *VMware Information Options*

Command Syntax and Usage
show virt vmware hello Displays Virtual Machine hello settings. For a sample output, see page 174. **Command mode:** All
show virt vmware hosts Displays a list of VMware hosts. For a sample output, see page 174. **Command mode:** All
show virt vmware showhost {<*host UUID*>**|**<*host IP address*>**|**<*host name*>**}** Displays detailed information about a specific VMware host. For a sample output, see page 175. **Command mode:** All
show virt vmware showvm {<*VM UUID*>**|**<*VM IP address*>**|**<*VM name*>**}** Displays detailed information about a specific Virtual Machine (VM). For a sample output, see page 176. **Command mode:** All
show virt vmware switchport-mapping Displays ESX Server - switchport mapping. For a sample output, see page 176. **Command mode:** All
show virt vmware vms Displays the UUIDs and the names of all VMware VMs. For a sample output, see page 176. **Command mode:** All

VMware Hello Information

The following command displays VM hello parameters:

show virt vmware hello

Command mode: All

```
Current Settings:
        Hello Disabled
        Hello timer: 23 seconds
        Hello ports: 13
        Hello address: 10.36.30.1
```

VMware Host Information

The following command displays VM host information:

show virt vmware hosts

Command mode: All

```
UUID                                    Name(s), IP Address

------------------------------------------------------------------------
80a42681-d0e5-5910-a0bf-bd23bd3f7803  127.12.41.30
3c2e063c-153c-dd11-8b32-a78dd1909a69  127.12.46.10
64f1fe30-143c-dd11-84f2-a8ba2cd7ae40  127.12.44.50
c818938e-143c-dd11-9f7a-d8defa4b83bf  127.12.46.20
fc719af0-093c-dd11-95be-b0adac1bcf86  127.12.46.30
009a581a-143c-dd11-be4c-c9fb65ff04ec  127.12.46.40
```

VM host information includes the following:

- UUID associated with the VMware host.
- Name or IP address of the VMware host.

The following command displays information for a specific VM host:

show virt vmware showhost {*<host UUID>***|***<host IP address>***|***<host name>***}**

Command mode: All

```
Vswitches available on the host:

        vSwitch0
        vSwitch1

Host physical nics:

Device    vSwitch                       MAC Address
------------------------------------------------------------
vmnic0    None                          5c:f3:fc:49:f0:e4
vmnic1    vSwitch0                      5c:f3:fc:49:f0:e6
vmnic2    None                          00:00:c9:da:f5:d8
vmnic3    vSwitch1                      00:00:c9:da:f5:dc
vusb0     None                          5e:f3:fc:4f:f0:e7

Port Groups and their vSwitches on the host:

        Lenovo_test                   vSwitch0
        VM Network                    vSwitch0
        Management Network            vSwitch0
        Lenovo_Default                vSwitch1
        Lenovo_test30                 vSwitch1
        Lenovo_test40                 vSwitch1
        VM Network 2                  vSwitch1
        Lenovo_test50                 vSwitch1
        Lenovo_unu                    vSwitch1

Detailed information about host and VM interfaces on this hypervisor:
-----------------------------------------------    ------------------
MAC Address         5c:f3:fc:49:f0:e6
Port                N/A
Type                VM Kernel
IP Address          10.241.32.131
Host Name           10.241.32.131
Host UUID           cab9df06-8fd7-3ecf-a4ba-f373ed60ad9d
vSwitch             vSwitch0
Port Group          Management Network
VLAN ID             0
...
```

VMware VM Information

The following command displays information for a specific Virtual Machine (VM):

show virt vmware showvm {<*VM UUID*>**|**<*VM IP address*>**|**<*VM name*>**}**

Command mode: All

```
MAC Address         00:50:56:a5:32:f7
Port                23
Type                Virtual Machine
VM vCenter Name     arch131_nfs_3
VM OS hostname      Not Available
VM IP Address       3.3.3.2
VM UUID             422547ad-0ef7-5992-1184-63aa9030377e
Current VM Host     10.241.32.131
vSwitch             vSwitch1
Port Group          Lenovo_Default
VLAN ID             0
```

The following command displays the UUIDs and the names of all the VMware VMs:

show virt vmware vms

Command mode: All

```
Rescanning data center. Please wait.
UUID                                 Name(s), IP Address
------------------------------------------------------------------------
42312c26-2a75-c05b-eed2-6d837ac46fdd  SNSC
4225801c-dfdb-061d-65e4-4e4860d6fbcf  arch2_06
42253440-6de7-7416-8a29-fb462114ead0  arch2_05
422f49df-bf88-e4d5-6cee-047a626029aa  arch2_4_clone
4225a4f2-3422-038f-77b5-6134f5fd00b6  arch_clone
422fddf6-b9c3-fb52-9eed-fb7ccab48ab8  WIN_iperf
422573e7-f2a1-373a-87ec-7f78d8313cca  linux
422f08f6-c3b1-a641-a44a-f2698a850f3c  IxVM008, localhost, 10.241.30.208
422f15d2-5e6e-88ef-689e-9af8e4c69c34  IxVM007, localhost, 10.241.30.207
422f54d3-55b5-3731-e8f1-62abac8a0911  IxVM006, localhost, 10.241.30.206
422f42d0-329e-aec2-99c8-2724aa26db7a  IxVM005, localhost, 10.241.30.205
...
```

VMware VM information includes the following:

- UUID associated with the VMware VM.
- Name or IP address of the VMware VM.

ESX Server - Switchport Mapping

The following command displays ESX Server - switchport mapping:

show virt vmware switchport-mapping

Command mode: All

```
ST 5 ==> 10.241.32.133 vmnic4
ST 5 ==> 10.241.32.133 vmnic5
23 ==> 10.241.32.131 vmnic3
```

EVB Information

The following commands display Edge Virtual Bridge (EVB) Virtual Station Interface (VDP) discovery and configuration information.

Table 75. *EVB Information Options*

Command Syntax and Usage
show virt evb profile Displays all EVB profile parameters. **Command mode:** All
show virt evb profile *<profile number>* **[ports]** Displays the selected EVB profile parameters. It can include ports. **Command mode:** All
show virt evb profile ports Displays all EVB profile parameters including ports. **Command mode:** All
show virt evb vdp tlv Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs). **Command mode:** All
show virt evb vdp vm Displays all associated Virtual Machines (VMs). For a sample output, see page 179. **Command mode:** All
show virt evb vsidb *<VSI database number (1)>* Displays Virtual Station Interface database information. **Command mode:** All
show virt evb vsitypes [mgrid *<0-255>***|typeid** *<1-16777215>***| |version** *<0-255>***]** Displays the current Virtual Station Interface Type database parameters. For a sample output, see page 178. **Command mode:** All

EVB VSIType Information

The following command displays VSITypes database parameters:

`show virt evb vsitypes`

Command mode: All

```
Time Since Last Poll: 0 days 0 hours 0 minutes 14 seconds
Time Since Last Update: 14 days 16 hours 29 minutes 18 seconds

Total number of VSIType entries : 69

INDEX : 1
----------------------------------
        Name :
        Type ID : 9
        Version : 1
        Manager ID : 1
        VLAN : 9, 50
        TxRate : 10000000
        TxBurst : 64
        RxRate : 10000000
        RxBurst : 64
         ACL Index: 1
                SRC MAC : 00:00:00:00:00:00
                SRC MAC MASK : 00:00:00:00:00:00
                DST MAC : ff:ff:ff:ff:ff:ff
                DST MAC MASK : ff:ff:ff:ff:ff:ff
                VLAN : 0 (0x000)
                Ether Type : 0x0800 (IPv4)
                SRC IP : 0.0.0.0
                SRC IP MASK : 0.0.0.0
                DST IP : 0.0.0.0
                DST IP MASK : 0.0.0.0
                TOS : 0 (0x00)
                ACL Action : deny
          ACL Index: 2
                SRC MAC : 00:00:00:00:00:00
                SRC MAC MASK : 00:00:00:00:00:00
                DST MAC : ff:ff:ff:ff:ff:ff
                DST MAC MASK : ff:ff:ff:ff:ff:ff
                VLAN : 0 (0x000)
                Ether Type : 0x0000
                ACL Action : permit
...

INDEX : 2
----------------------------------
        Name :
        Type ID : 20
        Version : 1
        Manager ID : 1
        VLAN : 10, 11, 12, 13, 14, 15, 16, 20
        TxRate : 10000000
        TxBurst : 64
        RxRate : 10000000
        RxBurst : 64
```

```
ACL Index: 1
               SRC MAC : 00:00:00:00:00:00
               SRC MAC MASK : 00:00:00:00:00:00
               DST MAC : ff:ff:ff:ff:ff:ff
               DST MAC MASK : ff:ff:ff:ff:ff:ff
               VLAN : 0 (0x000)
               Ether Type : 0x0800 (IPv4)
               SRC IP : 0.0.0.0
               SRC IP MASK : 0.0.0.0
               DST IP : 0.0.0.0
               DST IP MASK : 0.0.0.0
               TOS : 0 (0x00)
               ACL Action : deny
         ACL Index: 2
               SRC MAC : 00:00:00:00:00:00
               SRC MAC MASK : 00:00:00:00:00:00
               DST MAC : ff:ff:ff:ff:ff:ff
               DST MAC MASK : ff:ff:ff:ff:ff:ff
               VLAN : 0 (0x000)
               Ether Type : 0x0000
               ACL Action : permit
```

EVB VMs Information

The following command displays all active VMs:

`show virt evb vdp vm`

Command mode: All

```
Total number of VM Association entries : 2
TypeId     MAC         Vlan Port TxACL RxEntry ACLs
------ ----------------- ----- -------- ----- ------- -------
9     00:50:56:95:30:ec 50  13.1 250    251 252 253 254 255 256
70    00:50:56:a5:6e:e7 70  13.1 232    226 227 228 229 230 231
```

Networking Virtualization Information

The following table displays Networking Virtualization (NWV) information commands.

Table 76. *Networking Virtualization Information Commands*

Command Syntax and Usage
show nwv nsx-gw Displays VXLAN Gateway information. For a sample output, see page 181. **Command mode:** All
show nwv nsx-gw datapath [*<VxLAN VNID (1-16777216)>***]** Displays the VXLAN Gateway datapath configuration for all Virtual Extensible LAN (VXLAN) Virtual Networks or just for a specific Virtual Network. To view a sample output, see page 183. **Command mode:** All
show nwv nsx-gw mac-address [mcast-local|mcast-remote| |ucast-local|ucast-remote] Displays VXLAN Gateway Forwarding table information. o `mcast-local` displays information for local multicast MAC addresses o `mcast-remote` displays information for remote multicast MAC addresses o `ucast-local` displays information for local unicast MAC addresses o `ucast-remote` displays information for remote unicast MAC addresses To view a sample output, see page 182. **Command mode:** All
show nwv nsx-gw tunnels Displays VXLAN Gateway tunnels information. To view a sample output, see page 184. **Command mode:** All
show nwv nsx-gw virtual-network [*<VxLAN VNID (1-16777216)>***]** Displays VXLAN Gateway information for all Virtual Networks or for a specific Virtual Network. To view a sample output, see page 184. **Command mode:** All
show nwv nsx-gw virtual-port [*<port alias or number>***]** Displays VXLAN Gateway information for all virtual ports or for a specific virtual port. To view a sample output, see page 184. **Command mode:** All
show pki certificate Displays the host SSL certificate needed by the NSX Manager. To view a sample output, see page 185. **Command mode:** All

VXLAN Gateway Information

The following command displays VXLAN Gateway information:

`show nwv nsx-gw`

Command mode: All

```
NSX Gateway Information:
Status:                 Enabled
Gateway IP:             192.168.200.30
BFD Status:             Enabled

Controller Connections:
Idx  Type           Peer               State    Inact. ms  Backoff ms  Latest Method
---  -------------  -----------------  -------  ---------  ----------  ------------------
1    SSL (Active)   10.241.43.60:6640  ACTIVE   30000      8000        transact (comment)
2    SSL (Active)   10.241.43.61:6640  ACTIVE   30000      8000        monitor
3    SSL (Active)   10.241.43.62:6640  ACTIVE   30000      8000        transact (comment)

Physical Port Count: 4
VNI-VLAN Mappings Count: 254
--------------------------
Name         VNI       VLAN   Status
-----------  --------  ----   ------
7/1           5001     1      Up
              5002     2      Up
              5003     3      Up
              5004     4      Up
...
```

VXLAN Gateway FDB Information

The following command displays VXLAN Gateway Forwarding table information:

`show nwv nsx-gw mac-address`

Command mode: All

```
Local MAC Count: 1
VNI       MAC                Tunnel           Port   Vlan
--------  -----------------  ---------------  -----  ----
5001      00:50:56:81:39:d7  192.168.200.30   22/1   1301

Remote MAC Count: 4
VNI       MAC                Tunnel
--------  -----------------  ---------------
5001      52:54:00:0e:90:d0  192.168.200.15
5001      52:54:00:e1:f4:44  192.168.200.16
5002      52:54:00:ee:38:88  192.168.200.16
5002      52:54:00:ff:58:6a  192.168.200.15

Local Multicast MAC Count: 2
VNI       MAC                Tunnel
--------  -----------------  ---------------
5001      unknown-dst        192.168.200.30
5002      unknown-dst        192.168.200.30

Remote Multicast MAC Count: 2
VNI       MAC                Tunnel
--------  -----------------  ---------------
5001      unknown-dst        192.168.200.11
                             192.168.200.12
5002      unknown-dst        192.168.200.11
                             192.168.200.12
```

VXLAN Gateway Datapath Information

The following command displays VXLAN Gateway datapath information:

`show nwv nsx-gw datapath`

Command mode: All

```
VNID: 5001
--------------------------------------

Virtual Ports towards the Underlay Network:
Local IP Address   Port    VLAN   TAG
---------------   -----   ----   ---
192.168.200.30     7/1      981    Y

Unicast Virtual Ports towards the Overlay Network:
Local IP Address   Remote IP Address   Port    VLAN
---------------   -----------------   -----   ----
192.168.200.30     192.168.200.11      6/1      18
192.168.200.30     192.168.200.12      6/2      18

Multicast Virtual Ports towards the Overlay Network:
Local IP Address   Remote IP Address   Port    VLAN
---------------   -----------------   -----   ----
192.168.200.30     192.168.200.11      6/1      18
192.168.200.30     192.168.200.12      6/2      18

--------------------------------------
VNID: 5002
--------------------------------------

Virtual Ports towards the Underlay Network:
Local IP Address   Port    VLAN   TAG
---------------   -----   ----   ---
192.168.200.30     7/1      329    Y

Unicast Virtual Ports towards the Overlay Network:
Local IP Address   Remote IP Address   Port    VLAN
---------------   -----------------   -----   ----
192.168.200.30     192.168.200.11      6/1      18
192.168.200.30     192.168.200.12      6/2      18

Multicast Virtual Ports towards the Overlay Network:
Local IP Address   Remote IP Address   Port    VLAN
---------------   -----------------   -----   ----
192.168.200.30     192.168.200.11      6/1      18
192.168.200.30     192.168.200.12      6/2      18

...
```

VXLAN Gateway Tunnel Information

The following command displays VXLAN Gateway tunnel information:

`show nwv nsx-gw tunnels`

Command mode: All

```
Tunnel Count: 4
Local IP Address  Remote IP Address  Remote Type    Status
----------------  -----------------  -------------  ------
192.168.200.30    192.168.200.12     SN(backup)     Up
192.168.200.30    192.168.200.11     SN(active)     Up
192.168.200.30    192.168.200.15     VTEP           Up
192.168.200.30    192.168.200.16     VTEP           Up
```

VXLAN Gateway Virtual Network Information

The following command displays VXLAN Gateway Virtual Network information:

`show nwv nsx-gw virtual-network`

Command mode: All

```
Logical Network Count: 1025
VNI         name
----------  ------------------------------------
5001        5a0b3c29-c89b-4ba4-98d3-5e490ee7f4d8
5002        db60e4e8-d036-4a18-87f8-9e9a19be795b
5003        a40b3671-c853-4f38-ab40-408ce7bfa29d
5004        8025323a-745f-4729-9fff-06a2f7b3dfc5
...
```

VXLAN Gateway Virtual Port Information

The following command displays VXLAN Gateway Virtual Port information:

`show nwv nsx-gw virtual-port`

Command mode: All

```
Port     VNID      Remote TEP           VLAN(s)
-----    ------    --------------      --------
7/1 (A)  5001      LOCAL                     1
8/1 (A)  5002      LOCAL                     2
6/1 (N)  5001      192.168.200.11      MULTIPLE
6/1 (M)  5001      192.168.200.11      MULTIPLE
```

SSL Host Certificate Information

The following command displays the SSL Host Certificate needed by the NSX Manager:

`show pki certificate`

Command mode: All

```
-----BEGIN CERTIFICATE-----
MIID1DCCArygAwIBAgIUZoTano6P5tC3IMT9fhVPESU2Mz4wDQYJKoZIhvcNAQEL
BQAwgaMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEUMBIGA1UEBxMLU2FudGEg
Q2xhcmExKzApBgNVBAoTIkxlbm92byBOZXR3b3JraW5nIE9wZXJhdGluZyBTeXN0
ZW0xHDAaBgNVBAsTE05ldHdvcmsgRW5naW5lZXJpbmcxFTATBgNVBAMTDDEwLjI0
MS4zOS4xNDEPMA0GCSqGSIb3DQEJARYAMB4XDTExMDMxMTAwMDEyNloXDTIxMDMw
ODIzMDEyNlowgaMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEUMBIGA1UEBxML
U2FudGEgQ2xhcmExKzApBgNVBAoTIkxlbm92byBOZXR3b3JraW5nIE9wZXJhdGlu
ZyBTeXN0ZW0xHDAaBgNVBAsTE05ldHdvcmsgRW5naW5lZXJpbmcxFTATBgNVBAMT
DDEwLjI0MS4zOS4xNDEPMA0GCSqGSIb3DQEJARYAMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAtxm0y5AeoAm/Y5ji2rPcOq/FJE+kARfrrSkJm9eAcraQ
3rsHFIEAyRfgc8fAxgHMarx8bAElQHFWJQb6lYGRsWwJ07ZyNq4mhPIz9PJi943s
1mLhRz47uUEi6VyOdNe19Zplo30A6p04qqZlTYQOWpaAFU8IhStoNzYXfdsBuizj
exhhEcyg3lqAAEJ/t60hVPUGaUTFynfSU5O/BGClCYrn6UDOZ6qV7husnqPO5KMq
Pey1yYWWFBln2gvuWDPvj0V0Dr7G4xGT9WgSXaS9l3SXyRH2aOzlnRY4p6Qp0yDW
DDVBEVtQ4ZAVaoA/BFpAy1pL3k86MjXleWGxvFCJKQIDAQABMA0GCSqGSIb3DQEB
CwUAA4IBAQCeuRHnx9Kedjt2gZY4osZAv/e6MmWoOTHc7ocEoNyoXZW+2fWJSPbW
hKFLlHI6TLyxwFN8Kmwm92j1xYGhGHzD6ylYvmwcSUCW0aOOXlVcW1ITI5Z+Hwj7
Eu9RGuFNFDIRoBmRIQSnA3RnmgxQcF5YChifpGdgI6X9Et+7szNCbd1J4TQqvJZL
rhw3Owi/8N2SousUlK6eKXxYoHQR85vr9/XTemcvN2UT/1C+9sYzkjbYRzF60hr2
fyWMOjEJ+PvtOqrpJkZgx/jW4AERYEHYMJZ6hCwdnfGUA4j74xVE4FRnUi3zctte
1fuD8I8GYjccYEUK6lIldVqFOPxEwaTp
-----END CERTIFICATE-----
```

UFP Information

The following commands display information about Unified Fabric Port (UFP) settings.

Table 77. *UFP Information Options*

Command Syntax and Usage
show ufp information cdcp [port *<port alias or number>***]** Displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see page 188. **Command mode:** All
show ufp information getvlan *<VLAN ID (2-4094)>* Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID. **Command mode:** All
show ufp information port [*<port alias or number>***]** Displays UFP status for all physical ports or only for a specified physical port. Information includes wether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see page 188. **Command mode:** All
show ufp information qos [port *<port alias or number>* **[vport** *<1-8>***]]** Displays UFP Quality of Service (QoS) information, such as bandwidth allocation, Qos mode, priority, or host Class of Service (COS) control. For details, see page 189. **Command mode:** All
show ufp information tlvstat [port *<port alias or number>***]** o Displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see page 190. **Command mode:** All
show ufp information vlan [*<VLAN ID (1-4094)>***]** Displays ports and virtual ports associated to all configured VLANs or to a specified VLAN ID. For details, see page 192. **Command mode:** All
show ufp information vport [port *<port alias or number>* **[vport** *<1-8>***]]** Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see page 191. **Command mode:** All

Table 77. *UFP Information Options*

Command Syntax and Usage
show ufp [port *<port alias or number>* **[vport** *<1-8>* **[network|qos||evb]]]** Displays the UFP network and QoS settings applied on all ports or on specified physical or virtual ports. o `network` filters only network settings o `qos` filters only QoS network settings o `evb` filters only evb profile settings **Command mode:** All
show ufp {receive|transmit} {cap|cdcp|linkdown|linkup|prop} port *<port alias or number>* Displays received/transmitted Type-Length-Values for the specified ports. o `cap` displays the UFP Capability Discovery TLV o `cdcp` displays the UFP Channel Discovery and Configuration Protocol TLV o `linkdown` displays the UFP LINK-DOWN TLV o `linkup` displays the UFP LINK-UP TLV o `prop` displays the UFP NIC PROPS TLV For details, see page 193. **Command mode:** All

Port Information

The following command displays UFP port information:

`show ufp information port`

Command mode: All

```
Alias  Port  state  vPorts  link up  link down  mismatch  disabled
------ ----- ------ ------- -------- ---------- --------- --------
17     17    ena      2       2  3
18     18    dis      0
19     19    ena      2       2  3
20     20    ena      1       3
21     21    dis      2
22     22    ena      2       2  3
```

Port information includes the following for each physical port:

- Port alias
- Port number
- UFP state
- Number of virtual ports enabled
- Link status on each channel (up, down, mismatch or disabled)

CDCP Information

The following command displays S-Channel Discovery and Configuration Protocol information:

`show ufp information cdcp`

Command mode: All

```
1      : Channel Request
2      : Channel Request
3      :         TxSVIDs
4      :         TxSVIDs
5      :         Disable
6      :         Disable
7      :         Disable
8      :         Disable
9      :         Disable
10     :         Disable
...
```

CDCP information includes the following for each physical port:

- Whether there is a channel set up
- CDCP communication status for active channels

UFP QoS Information

The following command displays Quality of Service (QoS) information:

`show ufp information qos`

Command mode: All

```
UFP QOS:

  Port | Vport | Mode | Minbw% | Maxbw% | Prio | HstCtrl
-------------------------------------------------------
25     | 1     |  BW  | 25     | 100    |      |
       | 2     |  BW  | 25     | 100    |      |
       | 3     |  BW  | 25     | 100    |      |
       | 4     |  BW  | 25     | 100    |      |
-------------------------------------------------------
26     | 1     |  ETS |        |        | 0    | Dis
       | 2     |  ETS |        |        | 1    | Dis
       | 3     |  ETS |        |        | 2    | Dis
       | 4     |  ETS |        |        | 3    | Dis
       | 5     |  ETS |        |        | 4    | Dis
       | 6     |  ETS |        |        | 5    | Dis
       | 7     |  ETS |        |        | 0    | Dis
       | 8     |  ETS |        |        | 0    | Dis
...
```

QoS information includes the following:

- Physical port number
- Virtual port number
- QoS mode
- Minimum guaranteed bandwidth allocated
- Maximum bandwidth achievable
- 802.1q port priority
- Host Class of Service (COS) Control setting

TLV Status Information

The following command displays Type-Length-Values information:

`show ufp information tlvstat`

Command mode: All

```
1      :         Success
2      :         Success
3      :        Disabled
4      :        Disabled
5      :        Disabled
6      :        Disabled
7      :        Disabled
8      :        Disabled
9      :        Disabled
...
```

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

Virtual Port Information

The following command displays virtual port information:

`show ufp information vport`

Command mode: All

```
vPort          state   mode  svid defvlan deftag pvlan evb VLANs
-------------  -----  ------ ---- ------- ------ ----- --- ----------
        10.1    dis   tunnel 0      0      dis   dis   dis
        10.2    dis   tunnel 0      0      dis   dis   dis
        10.3    dis   tunnel 0      0      dis   dis   dis
        10.4    dis   tunnel 0      0      dis   dis   dis
        10.5    up    access 4006   20     dis   trunk dis  20
        10.6    up    access 4007   11     dis   host  dis  11
        10.7    dis   tunnel 0      0      dis   dis   dis
        10.8    dis   tunnel 0      0      dis   dis   dis
        12.1    dis   tunnel 0      0      dis   dis   dis
        12.2    up    trunk  4003   10     dis   prom  dis  10
        12.3    up    trunk  4004   21     dis   trunk dis  21   23
        12.4    dis   tunnel 0      0      dis   dis   dis
        12.5    dis   tunnel 0      0      dis   dis   dis
        12.6    dis   tunnel 0      0      dis   dis   dis
        12.7    dis   tunnel 0      0      dis   dis   dis
        12.8    dis   tunnel 0      0      dis   dis   dis
...
```

Virtual port information includes the following for each virtual port:

- Virtual port number
- Channel status
- Operating mode (trunk, access, tunnel, auto, or FCoE)
- S-channel VLAN ID
- Default VLAN ID
- Default VLAN ID tagging enforcement
- Private VLAN mode (disabled, trunk, host, or promiscuous)
- EVB Profile ID (for virtual ports in auto mode used by QBG)
- VLANs the virtual port is associated with

VLAN Information

The following command displays VLAN information:

`show ufp information vlan`

Command mode: All

```
VLAN
----
  14

vPort list:
 17.3

EXT Port list:
 41       42

INT Port list:
 18

UFP Port list:
 17       20       22

VMR Port list:

----
VLAN
----
 100

vPort list:
 20.3

EXT Port list:

INT Port list:

UFP Port list:
 20

VMR Port list:
 20
```

VLAN information includes the following for each VLAN:

- VLAN ID
- Associated virtual ports
- Associated external ports
- Associated internal ports
- Associated UFP ports

TLV Information

The following commands display TLV information:

`show ufp receive cap port` *<port alias or number>*

Command mode: All

```
UFP Capability Discovery TLV Received on port INTA2:
    tlv     : Type 127 Length 7 OUI 00-18-b1 Subtype 1
    version : Max 1 Oper 1
    cna     : Req 1 Oper 1 Res 0x00
    switch  : Cap 1 Oper 1 Res 0x00
```

UFP Capability Discovery TLV information includes the following:

- TLV type and length
- Lenovo Organizationally Unique Identifier
- TLV Subtype
- Max Version and Operation Version
- UFP CNA Status which include UFP Request and UFP Operation
- UFP Switch Status which includes UFP Capable and UFP Operation

`show ufp transmit cdcp port` *<port alias or number>*

Command mode: All

```
CDCP TLV Transmitted on port INTA2:
    tlv     : Type 127 Length 23 OUI 00-80-c2 Subtype 14
    local   : Role 0 SComp 1 Channel Cap 5
    SCID 1  : SVID 1
    SCID 2  : SVID 4002
    SCID 3  : SVID 4003
    SCID 4  : SVID 0
    SCID 5  : SVID 0
```

UFP Channel Discovery and Configuration Protocol TLV includes the following:

- TLV type and length
- Lenovo Organizationally Unique Identifier
- TLV Subtype
- Role bit
- S-Component bit
- Channel Cap
- Corresponding index/SVID pairs

show ufp transmit linkdown port *<port alias or number>*

Command mode: All

```
UFP LINK-DOWN TLV transmitted on port 14:
    Header  : Type 2 Length 3 Flags 0x0 Status 0x0
    SCID  :  2
```

```
UFP NIC-PROPS TLV transmitted on port 61:
    Header  : Type 1 Length 10 Flags 0x0 Status 0x0
    Props   : Channel Type 1 SCHED Type 0 Res 0x0 Num VLAN 0
    SCID  2 SVID  122 iSCSI 0 Host Pri 0 FCoE 0 TC  5 Min BW   0 Max BW 0
```

show ufp receive linkup port *<port alias or number>*

Command mode: All

```
UFP LINK-UP TLV received on port 59:
    Header  : Type 3 Length 3 Flags 0x1 Status 0x0
    SCID  :  2
```

show ufp receive prop port *<port alias or number>*

Command mode: All

```
UFP NIC-PROPS TLV received on port 59:
    Header  : Type 1 Length 10 Flags 0x1 Status 0x0
    Props   : Channel Type 1 SCHED Type 1 Res 0x0 Num VLAN 0
    SCID  2 SVID 4002 iSCSI 0 Host Pri 0 FCoE 0 TC 0 Min BW 25 Max BW 100
```

Converged Enhanced Ethernet Information

The following table describes the Converged Enhanced Ethernet (CEE) information options.

Table 78. *CEE Information Options*

Command Syntax and Usage
show cee global {ets|pfc} [information| |priority-group *<0-7, 15>***]** Displays the current global ETS or PFC parameters. o `information` displays global information o `priority-group` displays the current global Priority Group parameters **Command mode:** All
show cee information Displays all CEE information. **Command mode:** All
show cee information dcbx port *<port alias or number>* Displays all DCBX information for the specified port or range of ports. **Command mode:** All
show cee information pfc port *<port alias or number>* Displays all PFC information for the specified port or range of ports. **Command mode:** All

DCBX Information

The following table describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 79. *DCBX Information Options*

Command Syntax and Usage
show cee information dcbx port *<port alias or number>* Displays all DCBX information for the specified port or range of ports. **Command mode:** All
show cee information dcbx port *<port alias or number>* **app_proto** Displays information about the DCBX Application Protocol state machine on the specified port or range of ports. For details, see page 203. **Command mode:** All
show cee information dcbx port *<port alias or number>* **control** Displays information about the DCBX Control state machine for the specified port or range of ports. For details, see page 197. **Command mode:** All
show cee information dcbx port *<port alias or number>* **ets** Displays information about the DCBX ETS state machine for the specified port or range of ports. For details, see page 200. **Command mode:** All
show cee information dcbx port *<port alias or number>* **feature** Displays information about the DCBX Feature state machine for the specified port or range of ports. For details, see page 198. **Command mode:** All
show cee information dcbx port *<port alias or number>* **pfc** Displays information about the DCBX PFC state machine for the specified port or range of ports. For details, see page 202. **Command mode:** All

DCBX Control Information

The following command displays DCBX Control information:

`show cee information dcbx port` *<port alias or number>* **`control`**

Command mode: All

```
DCBX Port Control State-machine Info
================================================
Port       OperStatus OperVer MaxVer SeqNo AckNo
---------- ---------- ------- ------ ----- -----
1          enabled    0       0      0     0
2          enabled    0       0      0     0
3          enabled    0       0      0     0
4          enabled    0       0      2     1
5          enabled    0       0      0     0
6          enabled    0       0      0     0
7          enabled    0       0      0     0
8          enabled    0       0      0     0
9          enabled    0       0      0     0
10         enabled    0       0      0     0
11         enabled    0       0      0     0
12         enabled    0       0      0     0
13         enabled    0       0      0     0
14         enabled    0       0      0     0
15         enabled    0       0      0     0
16         enabled    0       0      0     0
...
```

DCBX Control information includes the following:

- Port number
- DCBX status (enabled or disabled)
- Operating version negotiated with the peer device
- Maximum operating version supported by the system
- Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
- Sequence number of the most recent DCB feature TLV that has been acknowledged

DCBX Feature Information

The following command displays DCBX Feature information:

`show cee information dcbx port` *<port alias or number>* **`feature`**

Command mode: All

```
DCBX Port Feature State-machine Info
================================================================================
Port Type    AdmState Will Advrt OpVer MxVer PrWill SeqNo Err OperMode Syncd
---- ------- -------- ---- ----- ----- ----- ------ ----- --- -------- -----
1    ETS     enabled  No   Yes   0     0     No     1     No  disabled No
1    PFC     enabled  No   Yes   0     0     No     1     No  disabled No
1    AppProt enabled  No   Yes   0     0     No     1     No  disabled No
2    ETS     enabled  No   Yes   0     0     No     1     No  disabled No
2    PFC     enabled  No   Yes   0     0     No     1     No  disabled No
2    AppProt enabled  No   Yes   0     0     No     1     No  disabled No
3    ETS     enabled  No   Yes   0     0     No     1     No  disabled No
3    PFC     enabled  No   Yes   0     0     No     1     No  disabled No
3    AppProt enabled  No   Yes   0     0     No     1     No  disabled No
4    ETS     enabled  No   Yes   0     0     Yes    2     No  enabled  Yes
4    PFC     enabled  No   Yes   0     0     Yes    2     No  enabled  Yes
4    AppProt enabled  No   Yes   0     0     Yes    2     No  enabled  Yes
5    ETS     enabled  No   Yes   0     0     No     1     No  disabled No
5    PFC     enabled  No   Yes   0     0     No     1     No  disabled No
5    AppProt enabled  No   Yes   0     0     No     1     No  disabled No
...
```

The following table describes the DCBX Feature information.

Table 80. *DCBX Feature Information Fields*

Parameter	Description
Port	Displays each port's number.
Type	Feature type
AdmState	Feature status (Enabled or Disabled)
Will	Willing flag status (Yes/True or No/Untrue)
Advrt	Advertisement flag status (Yes/True or No/Untrue)
OpVer	Operating version negotiated with the peer device
MxVer	Maximum operating version supported by the system
PrWill	Peer's Willing flag status (Yes/True or No/Untrue)
SeqNo	Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes
Err	Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange of configuration data with the peer.

Table 80. *DCBX Feature Information Fields*

Parameter	Description
OperMode	Operating status negotiated with the peer device (enabled or disabled)
Syncd	Synchronization status between this port and the peer (Yes or No)

DCBX ETS Information

The following command displays DCBX ETS information:

`show cee information dcbx port` *<port alias or number>* **`ets`**

Command mode: All

```
DCBX Port Priority Group - Priority Allocation Table
====================================================
Port   Priority PgIdDes PgIdOper PgIdPeer
------ -------- ------- -------- --------
1      0        PGID0   PGID0    PGID0
1      1        PGID0   PGID0    PGID0
1      2        PGID0   PGID0    PGID0
1      3        PGID1   PGID0    PGID0
1      4        PGID2   PGID0    PGID0
1      5        PGID2   PGID0    PGID0
1      6        PGID2   PGID0    PGID0
1      7        PGID2   PGID0    PGID0
2      0        PGID0   PGID0    PGID0
2      1        PGID0   PGID0    PGID0
2      2        PGID0   PGID0    PGID0
2      3        PGID1   PGID0    PGID0
2      4        PGID2   PGID0    PGID0
2      5        PGID2   PGID0    PGID0
2      6        PGID2   PGID0    PGID0
2      7        PGID2   PGID0    PGID0

DCBX Port Priority Group - Bandwidth Allocation Table
=====================================================
Port   PrioGrp BwDes BwOper BwPeer
------ ------- ----- ------ ------
1      0       10    0      0
1      1       50    0      0
1      2       40    0      0
2      0       10    0      0
2      1       50    0      0
2      2       40    0      0
3      0       10    0      0
3      1       50    0      0
3      2       40    0      0
```

The following table describes the DCBX ETS information.

Table 81. *DCBX Feature Information Fields*

Parameter	Description
DCBX Port Priority Group - Priority Allocation Table	
Port	Displays each port's number
Priority	Displays each port's priority
PgIdDes	Priority Group ID configured on this switch
PgIdOper	Priority Group negotiated with the peer (operating Priority Group).
PgIdPeer	Priority Group ID configured on the peer

Table 81. *DCBX Feature Information Fields (continued)*

Parameter	Description
DCBX Port Priority Group - Bandwidth Allocation Table	
Port	Displays each port's number
PrioGrp	Displays each port's priority group
BwDes	Bandwidth allocation configured on this switch
BwOper	Bandwidth allocation negotiated with the peer (operating bandwidth)
BwPeer	Bandwidth allocation configured on the peer

DCBX PFC Information

The following command displays DCBX Priority Flow Control (PFC) information:

`show cee information dcbx port` *<port alias or number>* **`pfc`**

Command mode: All

```
DCBX Port Priority Flow Control Table
=====================================
Port   Priority EnableDesr EnableOper EnablePeer
------ -------- ---------- ---------- ----------
1      0        disabled    disabled    disabled
1      1        disabled    disabled    disabled
1      2        disabled    disabled    disabled
1      3        enabled     disabled    disabled
1      4        disabled    disabled    disabled
1      5        disabled    disabled    disabled
1      6        disabled    disabled    disabled
1      7        disabled    disabled    disabled
2      0        disabled    disabled    disabled
2      1        disabled    disabled    disabled
2      2        disabled    disabled    disabled
2      3        enabled     disabled    disabled
2      4        disabled    disabled    disabled
2      5        disabled    disabled    disabled
2      6        disabled    disabled    disabled
2      7        disabled    disabled    disabled
3      0        disabled    disabled    disabled
```

DCBX PFC information includes the following:

- Port number
- 802.1p value
- **EnableDesr:** Status configured on this switch
- **EnableOper**: Status negotiated with the peer (operating status)
- **EnablePeer**: Status configured on the peer

DCBX Application Protocol Information

The following command displays DCBX Application Protocol information:

`show cee information dcbx port` *<port alias or number>* **`app_proto`**

Command mode: All

```
DCBX Application Protocol Table
===============================

FCoE Priority Information
=========================
Protocol ID               : 0x8906
Selector Field            : 0
Organizationally Unique ID: 0x1b21

Port   Priority EnableDesr EnableOper EnablePeer
------ -------- ---------- ---------- ----------
1      0        disabled    disabled    disabled
1      1        disabled    disabled    disabled
1      2        disabled    disabled    disabled
1      3        enabled     disabled    disabled
1      4        disabled    disabled    disabled
1      5        disabled    disabled    disabled
1      6        disabled    disabled    disabled
1      7        disabled    disabled    disabled
2      0        disabled    disabled    disabled
2      1        disabled    disabled    disabled
FIP Snooping Priority Information
=================================
Protocol ID               : 0x8914
Selector Field            : 0
Organizationally Unique ID: 0x1b21

Port   Priority EnableDesr EnableOper EnablePeer
------ -------- ---------- ---------- ----------
1      0        disabled    disabled    disabled
1      1        disabled    disabled    disabled
1      2        disabled    disabled    disabled
1      3        enabled     disabled    disabled
1      4        disabled    disabled    disabled
1      5        disabled    disabled    disabled
1      6        disabled    disabled    disabled
1      7        disabled    disabled    disabled
2      0        disabled    disabled    disabled
```

The following table describes the DCBX Application Protocol information.

Table 82. *DCBX Application Protocol Information Fields*

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: • 0 = Ethernet Type • 1 = TCP socket ID
Organizationally Unique ID	DCBX TLV identifier
Port	Port number
Priority	802.1p value
EnableDesr	Status configured on this switch
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

ETS Information

The following table describes the Enhanced Transmission Selection (ETS) information options.

Table 83. *ETS Information Options*

Command Syntax and Usage
show cee global ets information Displays global ETS information. **Command mode:** All

The following command displays ETS information:

show cee global ets information

Command mode: All

```
Global ETS information:

Number of COSq: 8

Mapping of 802.1p Priority to Priority Groups:

Priority  PGID  COSq
--------  ----  ----
    0       0     0
    1       0     0
    2       0     0
    3       1     1
    4       2     2
    5       2     2
    6       2     2
    7       2     2

Bandwidth Allocation to Priority Groups:

PGID  PG%  Description
----  ---  -----------
  0    10
  1    50
  2    40
```

Enhanced Transmission Selection (ETS) information includes the following:

- Number of Class of Service queues (COSq) configured
- 802.1p mapping to Priority Groups and Class of Service queues
- Bandwidth allocated to each Priority Group

PFC Information

The following table describes the Priority Flow Control (PFC) information options.

Table 84. *PFC Information Options*

Command Syntax and Usage
show cee port *<port alias or number>* **pfc** Displays PFC information. **Command mode:** All
show cee port *<port alias or number>* **pfc information** Displays PFC information. **Command mode:** All
show cee port *<port alias or number>* **pfc priority** *<0-7>* Displays PFC information. **Command mode:** All

The following command displays PFC information:

show cee port *<port alias or number>* **pfc information**

Command mode: All

```
PFC information for Port 1:

PFC - ON

Priority   State   Description
--------   -----   -----------
   0        Dis
   1        Dis
   2        Dis
   3        Ena
   4        Dis
   5        Dis
   6        Dis
   7        Dis
------------------------------------------------------------------------------
State - indicates whether PFC is Enabled/Disabled on a particular priority
```

FCoE Initialization Protocol Snooping Information

The following table describes the FIP Snooping information options.

Table 85. *FIP Snooping Information Options*

Command Syntax and Usage
show fcoe fips fcf Displays FCF learned (detected). **Command mode:** All
show fcoe fips fcoe Displays FCoE connections learned (detected). **Command mode:** All
show fcoe fips information Displays FIP Snooping information for all ports. **Command mode:** All
show fcoe fips port *<port alias or number>* **[information]** Displays FIP Snooping (FIPS) information for the specified port or ports, including a list of current FIPS ACLs. **Command mode:** All
show fcoe fips vlans Displays VLAN information. **Command mode:** All
show fcoe information Displays all current FCoE information. **Command mode:** All

Python Scripting Information

The following commands display Python Scripting Information.

Table 86. *Python Scripting Information Commands*

Command Syntax and Usage
show script Displays a list of all installed scripts. **Command mode:** All
show script *<script filename>* Displays the content of a specified script. **Command mode:** All
show script-log Displays a list of all script log files. **Command mode:** All
show script-log *<script log filename>* Displays the content of a specified script-log. **Command mode**: All
show scheduler job Displays detailed information of all currently scheduled jobs. For more information, see page 209. **Command mode**: All
show scheduler job cpu-limit Displays configured CPU usage limit value. **Command mode**: All
show scheduler job name *<job name>* Displays detailed information of a specified scheduled job. **Command mode**: All
show scheduler job running Displays detailed information of all currently running jobs. **Command mode**: All
show scheduler job time-limit Displays configured elapsed time limit value. **Command mode**: All

Scheduler Job Information

The following command displays detailed information of all current scheduled jobs:

`show scheduler job`

Command mode: All

```
Job name: "auto_image_upgrade"
  time event: absolute start time: 2013/11/20 14:30:0,
              interval: 43200 seconds
  action: "auto_image_upgrade.py" "10.20.8.8 group1"
------------------------------------------------------------------------
------------------------------------------------------------------------
Job name: "auto_image_upgrade"
State: idle
Previous process id: 0
Next execution time: 14:30:04 Thu Nov 21, 2013
Previous execution time: 02:30:00 Thu Nov 21, 2013
Previous user msec: 255
Previous sys msec: 16
Previous cpu usage: 7.59 (%)
Execution count:1
------------------------------------------------------------------------
------------------------------------------------------------------------
Job name: "monitor"
  syslog event: LINKUP
  action: "exe_ping.py"
------------------------------------------------------------------------
------------------------------------------------------------------------
Job name: "monitor"
State: idle
Previous process id: 0
Next execution time: NA
Previous execution time: Yet to be executed or completed
Previous user msec: 0
Previous sys msec: 0
Previous cpu usage: 0.0 (%)
Execution count:0
```

The following table describes the Scheduler Job information.

Table 87. *Scheduler Job Information Fields*

Parameter	Description
Job name	The name of the displayed scheduler job
State	Current scheduler job state (Idle/Running/Matched)
Matched state	The event was raised but a different job is already running, thus the event is put into the event queue.
Previous process id	The internal process ID of the thread that previously run the job
Next execution time	The timestamp when the job is scheduled to run

Table 87. *Scheduler Job Information Fields*

Parameter	Description
Previous execution time	The timestamp when the job was last executed
Previous user msec	The CPU time consumed by user owned threads on the previous job execution
Previous sys msec	The CPU time consumed by system owned threads on the previous job execution
Previous cpu usage	The CPU percentage consumed by Python Scripting process on the previous job execution
Execution count	The number of times the job was executed

Information Dump

The following command dumps switch information:

`show information-dump`

Command mode: All

Use the dump command to dump all switch information available (10K or more, depending on your configuration). This data is useful for tuning and debugging switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

Chapter 3. Statistics Commands

You can use the Statistics Commands to view switch performance statistics in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch statistics.

Table 88. *Statistics Commands*

Command Syntax and Usage
`show counters` Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see page 337. **Command mode:** All
`show layer3 counters` Displays Layer 3 statistics. **Command mode:** All
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. See page 333 for a sample output and a description of NTP Statistics. **Command mode:** All
`show ptp counters` Displays Precision Time Protocol Statistics. See page 335 for a sample output and a description of PTP Statistics. **Command mode:** All
`show snmp-server counters` Displays SNMP statistics. See page 329 for sample output. **Command mode:** All
`clear cpu` Clears all CPU utilization statistics. **Command mode:** Privileged EXEC
`clear counters` Clears all statistics for all interfaces. **Command mode:** Privileged EXEC
`clear interface port` *<port alias or number>* **`counters`** Clears all statistics for the specified port. **Command mode:** All
`clear mp-counters` Clears all MP-related statistics. **Command mode:** Privileged EXEC

Port Statistics

These commands display traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

Table 89. *Port Statistics Commands*

Command Syntax and Usage
show interface port *<port alias or number>* **bitrate-usage** Displays the traffic rate in kilobits per second. **Command mode:** All
show interface port *<port alias or number>* **bridging-counters** Displays bridging ("dot1") statistics for the port. See page 222 for sample output. **Command mode:** All
show interface port *<port alias or number>* **bridging-rate** Displays per-second bridging ("dot1") statistics for the port. **Command mode:** All
show interface port *<port alias or number>* **dot1x counters** Displays IEEE 802.1X statistics for the port. See page 217 for sample output. **Command mode:** All
show interface port *<port alias or number>* **egress-queue-counters [***<queue number (0-7)>***|drop]** Displays the total number of packets and bytes either successfully transmitted or dropped for each queue of the specified ports. o `queue number` filters the output to the specified queue number o `drop` lists only the queues with dropped traffic (non-zero counters for dropped packets/bytes counters) See page 233 for sample output. **Command mode:** All
show interface port *<port alias or number>* **egress-queue-rate [***<queue number (0-7)>***|drop]** Displays the number of packets and bytes per second either successfully transmitted or dropped for each queue of the specified ports. o `queue number` filters the output to the specified queue number o `drop` lists only the queues with dropped traffic (non-zero rates for dropped packets/bytes) See page 234 for sample output. **Command mode:** All

Table 89. *Port Statistics Commands (continued)*

Command Syntax and Usage
show interface port *<port alias or number>* **ethernet-counters** Displays Ethernet (“dot3”) statistics for the port. See page 223 for sample output. **Command mode:** All
show interface port *<port alias or number>* **ethernet-rate** Displays per-second Ethernet (“dot3”) statistics for the port. **Command mode:** All
show interface port *<port alias or number>* **interface-counters** Displays interface statistics for the port. See page 226 for sample output. **Command mode:** All
show interface port *<port alias or number>* **interface-rate** Displays per-second interface statistics for the port. **Command mode:** All
show interface port *<port alias or number>* **ip-counters** Displays IP statistics for the port. See page 229 for sample output. **Command mode:** All
show interface port *<port alias or number>* **ip-rate** Displays per-second IP statistics for the port. **Command mode:** All
show interface port *<port alias or number>* **link-counters** Displays link statistics for the port. See page 229 for sample output. **Command mode:** All
show interface port *<port alias or number>* **oam counters** Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port. **Command mode:** All
show interface port *<port alias or number>* **ptp-counters** Displays Precision Time Protocol statistics for the port. See page 335 for a sample output and a description of PTP Statistics. **Command mode:** All
show interface port *<port alias or number>* **rmon-counters** Displays Remote Monitoring (RMON) statistics for the port. See page 230 for sample output. **Command mode:** All

Table 89. *Port Statistics Commands (continued)*

Command Syntax and Usage
`show ip bootp-relay counters interface` *<port alias or number>* Displays BOOTP relay statistics for the port. See page 221 for sample output. **Command mode:** All
`clear counters` Clears statistics for all ports. **Command mode:** Privileged EXEC
`clear interfaces` Clears counters for all interfaces and queues. **Command mode:** Privileged EXEC
`clear interface port` *<port alias or number>* **`counters`** Clears all statistics for the port. **Command mode:** Privileged EXEC
`clear interface port` *<port alias or number>* **`egress-queue-counter`** Clears all QoS egress counters for the specified ports for all queues. **Command mode:** Privileged EXEC
`clear ip bootp-relay counters [interface` *<port alias or number>***`]`** Clears BOOTP relay statistics for a specific ports or all ports. **Command mode:** Privileged EXEC

802.1X Authenticator Statistics

Use the following command to display the 802.1X authenticator statistics of the selected port:

`show interface port` *<port alias or number>* **`dot1x counters`**

Command mode: All

```
Authenticator Statistics:
  eapolFramesRx          = 925
  eapolFramesTx          = 3201
  eapolStartFramesRx     = 2
  eapolLogoffFramesRx    = 0
  eapolRespIdFramesRx    = 463
  eapolRespFramesRx      = 460
  eapolReqIdFramesTx     = 1820
  eapolReqFramesTx       = 1381
  invalidEapolFramesRx   = 0
  eapLengthErrorFramesRx = 0
  lastEapolFrameVersion  = 1
  lastEapolFrameSource   = 00:01:02:45:ac:51
```

The following table describes the 802.1X authenticator statistics.

Table 90. *802.1X Authenticator Statistics of a Port*

Statistics	Description
eapolFramesRx	Total number of EAPOL frames received
eapolFramesTx	Total number of EAPOL frames transmitted
eapolStartFramesRx	Total number of EAPOL Start frames received
eapolLogoffFramesRx	Total number of EAPOL Logoff frames received
eapolRespIdFramesRx	Total number of EAPOL Response Identity frames received
eapolRespFramesRx	Total number of Response frames received
eapolReqIdFramesTx	Total number of Request Identity frames transmitted
eapolReqFramesTx	Total number of Request frames transmitted
invalidEapolFramesRx	Total number of invalid EAPOL frames received
eapLengthErrorFramesRx	Total number of EAP length error frames received
lastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
lastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

802.1X Authenticator Diagnostics

Use the following command to display the 802.1X authenticator diagnostics of the selected port:

`show interface port` *<port alias or number>* **`dot1x counters`**

Command mode: All

```
Authenticator Diagnostics:
  authEntersConnecting                = 1820
  authEapLogoffsWhileConnecting       = 0
  authEntersAuthenticating            = 463
  authSuccessesWhileAuthenticating    = 5
  authTimeoutsWhileAuthenticating     = 0
  authFailWhileAuthenticating         = 458
  authReauthsWhileAuthenticating      = 0
  authEapStartsWhileAuthenticating    = 0
  authEapLogoffWhileAuthenticating    = 0
  authReauthsWhileAuthenticated       = 3
  authEapStartsWhileAuthenticated     = 0
  authEapLogoffWhileAuthenticated     = 0
  backendResponses                    = 923
  backendAccessChallenges             = 460
  backendOtherRequestsToSupplicant    = 460
  backendNonNakResponsesFromSupplicant = 460
  backendAuthSuccesses                = 5
  backendAuthFails                    = 458
```

The following table describes the 802.1X authenticator diagnostics statistics.

Table 91. *802.1X Authenticator Diagnostics of a Port*

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhileConnecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEntersAuthenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
authSuccessesWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.

Table 91. *802.1X Authenticator Diagnostics of a Port (continued)*

Statistics	Description
authTimeoutsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.

Table 91. *802.1X Authenticator Diagnostics of a Port (continued)*

Statistics	Description
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
backendOtherRequests ToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNakResponses FromSupplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator.s chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

BootStrap Protocol Relay Statistics

Use the following command to display the BOOTP Relay statistics of the selected port:

`show ip bootp-relay counters interface` *<port alias or number>*

Command mode: All

```
BOOTP Relay statistics for port 1:

Requests received from client:        0
Requests relayed to server:           0
Requests relayed with option 82:      0
Requests dropped due to ...
  - relay not allowed:                0
  - no server or unreachable server:  0
  - packet or processing errors:      0
Replies received from server:         0
Replies relayed to client:            0
Replies dropped due to ...
  - packet or processing errors:      0
```

Bridging Statistics

Use the following command to display the bridging statistics of the selected port:

`show interface port` *<port alias or number>* **`bridging-counters`**

Command mode: All

```
Bridging statistics for port 1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

The following table describes the bridging statistics.

Table 92. *Bridging Statistics of a Port*

Statistics	Description
dot1PortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortOutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
dot1PortInDiscards	Count of valid frames received which were discarded (that is, filtered) by the Forwarding Process.
dot1TpLearnedEntry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

Ethernet Statistics

Use the following command to display the ethernet statistics of the selected port:

`show interface port` *<port alias or number>* **`ethernet-counters`**

Command mode: All

```
Ethernet statistics for port 1:
dot3StatsAlignmentErrors:                   0
dot3StatsFCSErrors:                         0
dot3StatsSingleCollisionFrames:             0
dot3StatsMultipleCollisionFrames:           0
dot3StatsLateCollisions:                    0
dot3StatsExcessiveCollisions:               0
dot3StatsInternalMacTransmitErrors:        NA
dot3StatsFrameTooLongs:                     0
dot3StatsInternalMacReceiveErrors:          0
```

The following table describes the ethernet statistics.

Table 93. *Ethernet Statistics of a Port*

Statistics	Description
dot3StatsAlignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `frameCheckError` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 93. *Ethernet Statistics of a Port (continued)*

Statistics	Description
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
dot3StatsMultipleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMac TransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3StatsCarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 93. *Ethernet Statistics of a Port (continued)*

Statistics	Description
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the `frameTooLong` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsInternalMac ReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsFrameTooLongs` object, the `dot3StatsAlignmentErrors` object, or the `dot3StatsFCSErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

Interface Statistics

Use the following command to display the interface statistics of the selected port:

`show interface port` *<port alias or number>* **`interface-counters`**

Command mode: All

```
Interface statistics for port 1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
FlowCtrlPkts:                      0                      0
PriFlowCtrlPkts:                   0                      0
Discards:                          0                      0
Errors:                            0                  21187


Ingress Discard reasons:              Egress Discard reasons:

VLAN Discards:                     0  HOL-blocking Discards:         0
Filter Discards:                   0  MMU Discards:                  0
Policy Discards:                   0  Cell Error Discards:           0
Non-Forwarding State:              0  MMU Aging Discards:            0
IBP/CBP Discards:                  0  Other Discards:                0
OBM LP packet discards:            0
OBM HP packet discards:            0
```

The following table describes the interface statistics.

Table 94. *Interface Statistics of a Port*

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sub-layer to a higher sub- layer, which were not addressed to a multicast or broadcast address at this sub-layer.
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher sub- layer, which were addressed to a broadcast address at this sub-layer.
ifInMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
ifInFlowControlPkts	The total number of flow control `pause` packets received on the interface.
ifInPriFlowControlPkts	The total number of priority flow control `pause` packets received on the interface.

Table 94. *Interface Statistics of a Port (continued)*

Statistics	Description
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed toa broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`.
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.
ifOutFlowControlPkts	The total number of flow control `pause` packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Table 94. *Interface Statistics of a Port (continued)*

Statistics	Description
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.
Filter Discards	Dropped by the Content Aware Engine (user-configured filter).
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
OBM LP packet discards	Number of low priority packets discarded because of oversubscription buffer management. Oversubscription is applicable only for packet size less than 200 bytes.
OBM HP packet discards	Number of high priority packets discarded because of oversubscription buffer management. Oversubscription is applicable only for packet size less than 200 bytes.
HOL-blocking Discards	Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of the Memory Management Unit.
Cell Error Discards	
MMU Aging Discards	
Other Discards	Discarded packets not included in any category.

Interface Protocol Statistics

Use the following command to display the interface protocol statistics of the selected port:

`show interface port` *<port alias or number>* **`ip-counters`**

Command mode: All

```
GEA IP statistics for port 1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

The following table describes the interface protocol statistics.

Table 95. *Interface Protocol Statistics of a Port*

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHeaderErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Link Statistics

Use the following command to display the link statistics of the selected port:

`show interface port` *<port alias or number>* **`link-counters`**

Command mode: All

```
Link statistics for port 1:
linkStateChange:       1
```

The following table describes the link statistics.

Table 96. *Link Statistics of a Port*

Statistics	Description
linkStateChange	The total number of link state changes.

RMON Statistics

Use the following command to display the Remote Monitoring (RMON) statistics of the selected port:

`show interface port` *<port alias or number>* **`rmon-counters`**

Command mode: All

```
RMON statistics for port 1:
etherStatsDropEvents:                NA
etherStatsOctets:                   538
etherStatsPkts:                       4
etherStatsBroadcastPkts:              1
etherStatsMulticastPkts:              3
etherStatsCRCAlignErrors:             0
etherStatsUndersizePkts:              0
etherStatsOversizePkts:               0
etherStatsFragments:                  0
etherStatsJabbers:                    0
etherStatsCollisions:                 0
etherStatsPkts64Octets:               3
etherStatsPkts65to127Octets:          0
etherStatsPkts128to255Octets:         0
etherStatsPkts256to511Octets:         1
etherStatsPkts512to1023Octets:        0
etherStatsPkts1024to1518Octets:       0
```

The following table describes the RMON statistics.

Table 97. *RMON Statistics of a Port*

Statistics	Description
etherStatsDropEvents	The total number of packets received that were dropped because of system resource constraints.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsPkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.

Table 97. *RMON Statistics of a Port (continued)*

Statistics	Description
etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).

Table 97. *RMON Statistics of a Port (continued)*

Statistics	Description
etherStatsPkts128to255Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

QoS Queue Counter-Based Statistics

Use the following command to display the counter-based QoS queue statistics of the selected port:

`show interface port` *<port alias or number>* **`egress-queue-counters`**

Command mode: All

```
QoS statistics for port 1:
QoS Queue 0:
    Tx Packets:                            31
    Dropped Packets:                        0
    Tx Bytes:                           10444
    Dropped Bytes:                          0
QoS Queue 1:
    Tx Packets:                             0
    Dropped Packets:                        0
    Tx Bytes:                               0
    Dropped Bytes:                          0
QoS Queue 2:
    Tx Packets:                             0
    Dropped Packets:                        0
    Tx Bytes:                               0
    Dropped Bytes:                          0
QoS Queue 3:
    Tx Packets:                             0
    Dropped Packets:                        0
    Tx Bytes:                               0
    Dropped Bytes:                          0
...
QoS Queue 7:
    Tx Packets:                           900
    Dropped Packets:                        0
    Tx Bytes:                           64320
    Dropped Bytes:                          0
```

The following table describes the counter-based QoS queue statistics.

Table 98. *QoS Queue Counter-Based Statistics of a Port*

Statistics	Description
Tx Packets	Total number of successfully transmitted packets for the QoS queue
Dropped Packets	Total number of dropped packets for the QoS queue
Tx Bytes	Total number of successfully transmitted bytes for the QoS queue
Dropped Bytes	Total number of dropped bytes for the QoS queue

QoS Queue Rate-Based Statistics

Use the following command to display the rate-based QoS queue statistics of the selected port:

`show interface port` *<port alias or number>* **`egress-queue-rate`**

Command mode: All

```
QoS Rate for port 1:
QoS Queue 0:
    Tx Packets:                           5
    Dropped Packets:                      0
    Tx Bytes:                           363
    Dropped Bytes:                        0
QoS Queue 1:
    Tx Packets:                           0
    Dropped Packets:                      0
    Tx Bytes:                             0
    Dropped Bytes:                        0
QoS Queue 2:
    Tx Packets:                           0
    Dropped Packets:                      0
    Tx Bytes:                             0
    Dropped Bytes:                        0
QoS Queue 3:
    Tx Packets:                           0
    Dropped Packets:                      0
    Tx Bytes:                             0
    Dropped Bytes:                        0
...
QoS Queue 7:
    Tx Packets:                           0
    Dropped Packets:                      0
    Tx Bytes:                             0
    Dropped Bytes:                        0
```

The following table describes the rate-based QoS queue statistics.

Table 99. *QoS Queue Rate-Based Statistics of a Port*

Statistics	Description
Tx Packets	Number of successfully transmitted packets per second for the QoS queue
Dropped Packets	Number of dropped packets per second for the QoS queue
Tx Bytes	Number of successfully transmitted bytes per second for the QoS queue
Dropped Bytes	Number of dropped bytes per second for the QoS queue

Link Aggregation Group (LAG) Statistics

The following commands display Link Aggregation Group (LAG) statistics:

Table 100. *LAG Statistics Commands*

Command Syntax and Usage
show interface portchannel *<1-144>* **interface-counters** Displays interface statistics for the LAG. **Command mode:** All
clear interface portchannel *<1-144>* **counters** Clears all the statistics on the selected LAG. **Command mode:** Privileged EXEC

Layer 2 Statistics

The following commands display Layer 2 statistics:

Table 101. *Layer 2 Statistics Commands*

Command Syntax and Usage
show hotlinks counters Displays Hot Links statistics. See page 241 for sample output. **Command mode:** All
show interface port *<port alias or number>* **lacp counters** Displays Link Aggregation Control Protocol (LACP) statistics. See page 240 for sample output. **Command mode:** All
show interface port *<port alias or number>* **lldp counters** Displays LLDP statistics. See page 242 for sample output. **Command mode:** All
show mac-address-table counters Displays FDB statistics. See page 239 for sample output. **Command mode:** All
show mac-address-table counters all Displays all FDB statistics for all FDB entries. **Command mode:** All
show mac-address-table counters interface port *<port alias or number>* Displays FDB statistics for a particular port. **Command mode:** All
show mac-address-table counters portchannel *<1-144>* Displays all FDB statistics for a particular Link Aggregation Group (LAG). **Command mode:** All
show mac-address-table counters state {unknown|forward| |trunk} Displays all FDB statistics for a particular state. **Command mode:** All
show mac-address-table counters static Displays all FDB statistics for all static FDB entries. **Command mode:** All

Table 101. *Layer 2 Statistics Commands*

Command Syntax and Usage
show mac-address-table counters unicast Displays all FDB statistics for all Unicast FDB entries. **Command mode:** All
show mac-address-table counters vlan *<VLAN ID (1-4094)>* Displays all FDB statistics on a single VLAN. **Command mode:** All
show oam counters Displays OAM statistics. See page 244 for sample output. **Command mode:** All
show spanning-tree statistics Displays all Spanning Tree Protocol (STP) statistics. See page 243 for sample output. **Command mode**: All
show spanning-tree statistics port *<port alias or number>* Displays STP statistics for the specified port. See page 243 for sample output. **Command mode**: All
show spanning-tree statistics stp *<1-128>* Displays STP statistics for the specified Spanning Tree Group (STG). See page 243 for sample output. **Command mode**: All
show vlag statistics Displays all vLAG statistics. See page 245 for sample output. **Command mode:** All
clear hotlinks Clears all Hot Links statistics. **Command mode:** Privileged EXEC
clear interface port *<port alias or number>* **lacp counters** Clears Link Aggregation Control Protocol (LACP) statistics. **Command mode:** Privileged EXEC
clear interface port *<port alias or number>* **lldp-counters** Clears Link Layer Detection Protocol (LLDP) statistics for the specified port. **Command mode:** Privileged EXEC
clear mac-address-table counters Clears FDB statistics. **Command mode:** Privileged EXEC

Table 101. *Layer 2 Statistics Commands*

Command Syntax and Usage
clear spanning-tree statistics Clears all STP statistics. **Command mode**: Privileged EXEC
clear vlag statistics Clears all vLAG statistics. **Command mode:** Privileged EXEC

FDB Statistics

Use the following command to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches:

`show mac-address-table counters`

Command mode: All

```
FDB statistics:
 current:           83   hiwat:             855
```

FDB statistics are described in the following table:

Table 102. *Forwarding Database Statistics*

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

`show interface port` *<port alias or number>* **`lacp counters`**

Command mode: All

```
Port 1:
 -------------------------------------
 Valid LACPDUs received:         - 870
 Valid Marker PDUs received:     - 0
 Valid Marker Rsp PDUs received: - 0
 Unknown version/TLV type:       - 0
 Illegal subtype received:       - 0
 LACPDUs transmitted:            - 6031
 Marker PDUs transmitted:        - 0
 Marker Rsp PDUs transmitted:    - 0
```

Link Aggregation Control Protocol (LACP) statistics are described in the following table:

Table 103. *LACP Statistics*

Statistic	Description
Valid LACPDUs received	Total number of valid LACP data units received.
Valid Marker PDUs received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs received	Total number of valid LACP marker response data units received.
Unknown version/TLV type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal subtype received	Total number of LACP data units with an illegal subtype received.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs transmitted	Total number of LACP marker response data units transmitted.

Hotlinks Statistics

Use the following command to display Hot Links statistics:

`show hotlinks counters`

Command mode: All

```
Hot Links Trigger Stats:

Trigger 1 statistics:
    Trigger Name: Trigger 1
    Master active:           0
    Backup active:           0
    FDB update:              0   failed: 0
```

The following table describes the Hotlinks statistics:

Table 104. *Hotlinks Statistics*

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

LLDP Port Statistics

Use the following command to display LLDP statistics:

`show interface port` *<port alias or number>* **`lldp counters`**

Command mode: All

```
LLDP Port 1 Statistics
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Frames Transmitted          : 0
Frames Received             : 0
Frames Received in Errors   : 0
Frames Discarded            : 0
TLVs Unrecognized           : 0
Neighbors Aged Out          : 0
```

The following table describes the LLDP port statistics:

Table 105. *LLDP port Statistics*

Statistic	Description
`Frames Transmitted`	Total number of LLDP frames transmitted.
`Frames Received`	Total number of LLDP frames received.
`Frames Received in Errors`	Total number of LLDP frames that had errors.
`Frames Discarded`	Total number of LLDP frames discarded.
`TLVs Unrecognized`	Total number of unrecognized TLV (Type, Length, and Value) fields received.
`Neighbors Aged Out`	Total number of neighbor devices that have had their LLDP information aged out.

Spanning Tree Statistics

Use the following command to display Spanning Tree Protocol (STP) statistics:

`show spanning-tree statistics`

Command mode: All

```
Spanning-tree group: 1
  Port    RxBpdu      TxBpdu        RxTCN         LastTCNRx       TxTCN        LastTCNTx
------  ----------  ----------  ----------  ------------------ ---------- ------------------
17              28      212246          22  13:53:41  7-15-2016     210286 11:35:54  7-20-2016
18              13      212244           7  13:53:18  7-15-2016     210289 11:35:54  7-20-2016
20          212328      210259      181570  11:35:55  7-20-2016     210257 11:35:54  7-20-2016
21          212326           2      210366  11:35:54  7-20-2016          1 13:33:07  7-15-2016
22          238753      423006      204170  11:35:54  7-20-2016     420536 11:35:54  7-20-2016
23          232365      423004      204612  11:35:54  7-20-2016     420530 11:35:54  7-20-2016
24          240073      423000      199662  11:35:53  7-20-2016     420528 11:35:54  7-20-2016
-------------------------------------------------------------------------------------------
Spanning-tree group: 23
  Port    RxBpdu      TxBpdu        RxTCN         LastTCNRx       TxTCN        LastTCNTx
------  ----------  ----------  ----------  ------------------ ---------- ------------------
11              39      211499           5  14:01:02  7-15-2016        101  2:11:41  7-20-2016
12              36      211499           2  13:53:06  7-15-2016        104  2:11:41  7-20-2016
13              36      211497           2  13:53:06  7-15-2016        104  2:11:41  7-20-2016
14              36      211481           2  13:53:06  7-15-2016        104  2:11:41  7-20-2016
15              36      211497           2  13:53:06  7-15-2016        104  2:11:41  7-20-2016
```

Use the following command to display STP statistics for a specific port:

`show spanning-tree statistics port` *<port alias or number>*

Command mode: All

```
Port: 17
  stg    RxBpdu     TxBpdu      RxTCN        LastTCNRx         TxTCN        LastTCNTx
------ ---------- ---------- ---------- ------------------ ---------- ------------------
 1             28     212329         22 13:53:41  7-15-2016     210369 11:38:41  7-20-2016
-------------------------------------------------------------------------------------------
   Dropped Bpdu counter: 28
```

Use the following command to display STP statistics for a specific Spanning Tree Group (STG):

`show spanning-tree statistics stp` *<1-128>*

Command mode: All

```
Spanning-tree group: 1
  Port    RxBpdu      TxBpdu        RxTCN         LastTCNRx       TxTCN        LastTCNTx
------  ----------  ----------  ----------  ------------------ ---------- ------------------
17              28      212246          22  13:53:41  7-15-2016     210286 11:35:54  7-20-2016
18              13      212244           7  13:53:18  7-15-2016     210289 11:35:54  7-20-2016
20          212328      210259      181570  11:35:55  7-20-2016     210257 11:35:54  7-20-2016
21          212326           2      210366  11:35:54  7-20-2016          1 13:33:07  7-15-2016
22          238753      423006      204170  11:35:54  7-20-2016     420536 11:35:54  7-20-2016
23          232365      423004      204612  11:35:54  7-20-2016     420530 11:35:54  7-20-2016
24          240073      423000      199662  11:35:53  7-20-2016     420528 11:35:54  7-20-2016
```

OAM Statistics

Use the following command to display OAM statistics:

`show oam counters`

Command mode: All

```
OAM statistics on port 1
----------------------------------------
Information OAMPDU Tx :      0
Information OAMPDU Rx :      0
Unsupported OAMPDU Tx :      0
Unsupported OAMPDU Tx :      0

Local faults
-------------
    0 Link fault records
    0 Critical events
    0 Dying gasps

Remote faults
-------------
    0 Link fault records
    0 Critical events
    0 Dying gasps
```

OAM statistics include the following:

- Total number of OAM Protocol Data Units (OAMPDU) transmitted and received.
- Total number of unsupported OAM Protocol Data Units (OAMPDU) transmitted and received.
- Local faults detected.
- Remote faults detected.

vLAG Statistics

The following table describes the vLAG statistics commands:

Table 106. *vLAG Statistics Options*

Command Syntax and Usage
show vlag statistics Displays all vLAG statistics. See page 245 for sample output. **Command mode:** All
show vlag isl-statistics Displays vLAG ISL statistics for the selected port. See page 246 for sample output. **Command mode:** All
clear vlag statistics Clears all vLAG statistics. **Command mode:** Privileged EXEC

Use the following command to display vLAG statistics:

show vlag statistics

Command mode: All

```
vLAG PDU sent:
Role Election:         10        System Info:           7
Peer Instance Enable: 624        Peer Instance Disable: 52
FDB Dynamic Add:      166079     FDB Dynamic Del:       33856
FDB Inactive Add:     0          FDB Inactive Del:      0
Health Check:         4665       ISL Hello:             2126
Other:                0          Unknown:               0


vLAG PDU received:
Role Election:         11        System Info:           6
Peer Instance Enable: 572        Peer Instance Disable: 52
FDB Dynamic Add:      122523     FDB Dynamic Del:       38991
FDB Inactive Add:     7200       FDB Inactive Del:      0
Health Check:         4656       ISL Hello:             2114
Other:                0          Unknown:               0


vLAG IGMP packets forwarded:
IGMP Reports:         0
IGMP Leaves:          0
```

The following table describes the vLAG statistics:

Table 107. *VLAG Statistics*

Statistic	Description
`Role Election`	Total number of vLAG PDUs sent/received for role elections.
`System Info`	Total number of vLAG PDUs sent/received for getting system information.
`Peer Instance Enable`	Total number of vLAG PDUs sent/received for enabling peer instance.
`Peer Instance Disable`	Total number of vLAG PDUs sent/received for disabling peer instance.
`FDB Dynamic Add`	Total number of vLAG PDUs sent/received for addition of FDB dynamic entry.
`FDB Dynamic Del`	Total number of vLAG PDUs sent/received for deletion of FDB dynamic entry.
`FDB Inactive Add`	Total number of vLAG PDUs sent/received for addition of FDB inactive entry.
`FDB Inactive Del`	Total number of vLAG PDUs sent/received for deletion of FDB inactive entry.
`Health Check`	Total number of vLAG PDUs sent/received for health checks.
`ISL Hello`	Total number of vLAG PDUs sent/received for ISL `hello`.
`Other`	Total number of vLAG PDUs sent/received for other reasons.
`Unknown`	Total number of vLAG PDUs sent/received for unknown operations.

vLAG ISL Statistics

Use the following command to display vLAG statistics:

`show vlag isl-statistics`

Command mode: All

```
                                In Counter        Out Counter
Octets:                          2755820              2288
Packets:                           21044                26
```

ISL statistics include the total number of octets received/transmitted, and the total number of packets received/transmitted over the Inter-Switch Link (ISL).

Layer 3 Statistics

The following commands display Layer 3 statistics:

Table 108. *Layer 3 Statistics Commands*

Command Syntax and Usage
show [ip] arp counters Displays Address Resolution Protocol (ARP) statistics. See page 262 for sample output. **Command mode:** All
show ip arp inspection statistics [vlan *<VLAN ID (1-4094)>***]** Displays Dynamic ARP Inspection statistics. See page 262 for sample output. **Command mode:** All
show ip counters Displays Internet Protocol (IP) statistics. See page 253 for sample output. **Command mode:** All
show ipv6 counters Displays Internet Protocol version 6 (IPv6) statistics. See page 255 for sample output. **Command mode:** All
show ip dhcp snooping counters Displays Dynamic Host Control Protocol (DHCP) Snooping statistics. **Command mode:** All
show ip dns counters Displays Domain Name System (DNS) statistics. See page 263 for sample output. **Command mode:** All
show ip gea [bucket *<IP address>***|ecmp** *<IP address> <IP netmask>***]** Displays Gigabit Ethernet Aggregators (GEA) statistics. GEA statistics are used by service and support personnel. **Command mode:** All
show ip icmp counters Displays Internet Control Message Protocol (ICMP) statistics. See page 264 for sample output. **Command mode:** All
show ip igmp counters Displays Internet Group Management Protocol (IGMP) statistics. See page 269 for sample output. **Command mode:** All

Table 108. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
show ip igmp port *<port alias or number>* **counter** Displays port IGMP statistics. **Command mode**: All
show ip igmp vlan *<VLAN ID (1-4094)>* **counter** Displays IGMP statistics for a specific VLAN. See page 269 for sample output. **Command mode:** All
show ipv6 mld counters Displays MLD statistics. See page 272 for sample output. **Command mode:** All
show ip nat statistics Displays Network Address Translation (NAT) statistics. **Command mode:** All
show ipv6 neighbors counters Displays IPv6 Neighbor Cache statistics. **Command mode**: All
show ip ospf counters Displays Open Shortest Path First (OSPF) statistics. See page 275 for sample output. **Command mode:** All
show ipv6 ospf counters Displays Open Shortest Path First version 3 (OSPFv3) statistics. See page 280 for sample output. **Command mode:** All
show ip pim counters Displays Protocol Independent Multicast (PIM) statistics for all configured PIM interfaces. See page 285 for sample output. **Command mode:** All
show ip pim interface {*<1-126>***|loopback** *<1-5>***|port** *<port alias or number>***} counters** Displays PIM statistics for the selected interface. **Command mode:** All
show ip pim mroute count Displays statistics of various multicast entry types. **Command mode:** All

Table 108. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
`show ip policy statistics` Displays statistics for the current routing policy. **Command mode:** All
`show ip rip counters` Displays Routing Information Protocol (RIP) statistics. See page 286 for sample output. **Command mode:** All
`show ip route counters` Displays IPv4 route statistics. See page 260 for sample output. **Command mode:** All
`show ipv6 route counters` Displays IPv6 route statistics. See page 261 for sample output. **Command mode:** All
`show ip slp counters` Displays Service Location Protocol (SLP) statistics. **Command mode**: All
`show ip tcp counters` Displays Transmission Control Protocol (TCP) statistics. See page 266 for sample output. **Command mode:** All
`show ip tenant` *<tenant ID (1-30)>* **`info`** Displays tenant statistics. **Command mode**: All
`show ip udp counters` Displays User Datagram Protocol (UDP) statistics. See page 268 for sample output. **Command mode:** All
`show ip vrrp counters` When virtual routers are configured, you can display the protocol statistics for Virtual Router Redundancy Protocol (VRRP). See page 284 for sample output. **Command mode:** All
`show layer3 counters` Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode:** All

Table 108. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
clear ip arp counters Clears Address Resolution Protocol (ARP) statistics. **Command mode:** Privileged EXEC
clear ip arp inspection statistics [vlan *<VLAN ID (1-4094)>***]** Clears Dynamic ARP Inspection statistics. **Command mode:** Privileged EXEC
clear ip counters Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. **Command mode:** Privileged EXEC
clear ipv6 counters Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics. **Command mode:** Privileged EXEC
clear ip dhcp snooping counters Clears DHCP Snooping statistics. **Command mode:** Privileged EXEC
clear ip dns counters Clears Domain Name System (DNS) statistics. **Command mode:** Privileged EXEC
clear ip icmp counters Clears Internet Control Message Protocol (ICMP) statistics. **Command mode:** Privileged EXEC
clear ip igmp [*<VLAN ID (1-4094)>***] counters** Clears all IGMP statistics. The `vlan` option clears IGMP statistics only for a specific VLAN. **Command mode:** Privileged EXEC
clear ipv6 mld counters Clears MLD statistics. **Command mode:** Privileged EXEC
clear ip nat statistics Clears NAT statistics. **Command Mode**: Privileged EXEC
clear ipv6 neighbors counters Clears all IPv6 Neighbor Cache statistics from switch memory. **Command mode**: Privileged EXEC

Table 108. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
clear ip ospf counters Clears Open Shortest Path First (OSPF) statistics. **Command mode:** Privileged EXEC
clear ipv6 ospf counters Clears Open Shortest Path First version 3 (OSPFv3) statistics. **Command mode:** Privileged EXEC
clear ip pim counters Clears PIM statistics for all interfaces. **Command mode:** Privileged EXEC
clear ip pim interface {*<interface number>***|port** *<port alias or number>***} counters** Clears PIM statistics on the selected interface. **Command mode**: Privileged EXEC
clear ip rip counters Clears Routing Information Protocol (RIP) statistics. **Command mode:** Privileged EXEC
clear ip route counters Clears IPv4 route statistics. **Command mode:** Privleged EXEC
clear ipv6 route counters Clears IPv6 route statistics. **Command mode:** Privileged EXEC
clear ip slp counters Clears SLP statistics. **Command mode:** Privileged EXEC
clear ip tcp counters Clears Transmission Control Protocol (TCP) statistics. **Command mode:** Privileged EXEC
clear ip tenant counters *<tenant ID (1-30)>* Clears tenant statistics. **Command mode**: Privileged EXEC

Table 108. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
clear ip udp counters Clears User Datagram Protocol (UDP) statistics. **Command mode:** Privileged EXEC
clear ip vrrp counters Clears VRRP statistics. **Command mode:** Privileged EXEC

IPv4 Statistics

The following command displays IPv4 statistics:

`show ip counters`

Command mode: All

```
IP statistics:
ipInReceives:              0   ipInHdrErrors:           0
ipInAddrErrors:            0
ipInUnknownProtos:         0   ipInDiscards:            0
ipInDelivers:              0   ipOutRequests:        1274
ipOutDiscards:             0
ipDefaultTTL:            255
```

Use the following command to clear IPv4 statistics:

`clear ip counters`

Table 109. *IPv4 Statistics*

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

Table 109. *IPv4 Statistics (continued)*

Statistics	Description
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipDefaultTTL	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.

IPv6 Statistics

The following command displays IPv6 statistics:

`show ipv6 counters`

Command mode: All

```
    IPv6 Statistics
    ***************
144  Rcvd          0    HdrErrors     0    TooBigErrors
0    AddrErrors    0    FwdDgrams     0    UnknownProtos
0    Discards      144  Delivers      130  OutRequests
0    OutDiscards   0    OutNoRoutes   0    ReasmReqds
0    ReasmOKs      0    ReasmFails
0    FragOKs       0    FragFails     0    FragCreates
7    RcvdMCastPkt  2    SentMcastPkts 0    TruncatedPkts
0    RcvdRedirects 0    SentRedirects
    ICMP Statistics
    ***************
    Received :
33  ICMPPkts     0 ICMPErrPkt      0 DestUnreach  0 TimeExcds
0   ParmProbs    0 PktTooBigMsg    9 ICMPEchoReq  10 ICMPEchoReps
0   RouterSols   0 RouterAdv       5 NeighSols    9 NeighAdv
0   Redirects    0 AdminProhib     0 ICMPBadCode
    Sent :
19  ICMPMsgs     0 ICMPErrMsgs     0 DstUnReach   0 TimeExcds
0   ParmProbs    0 PktTooBigs      10 EchoReq     9 EchoReply
0   RouterSols   0 RouterAdv       11 NeighSols   5 NeighborAdv
0   RedirectMsgs 0 AdminProhibMsgs
    UDP statistics
    **************
    Received :
0 UDPDgrams    0 UDPNoPorts       0 UDPErrPkts
    Sent :
0 UDPDgrams
```

Use the following command to clear IPv6 statistics:

`clear ipv6 counters`

Command mode: Privileged EXEC

The following table describes the IPv6 statistics.

Table 110. *IPv6 Statistics*

Statistic	Description
Rcvd	Number of datagrams received from interfaces, including those received in error.
HdrErrors	Number of datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
TooBigErrors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.

Table 110. *IPv6 Statistics (continued)*

Statistic	Description
AddrErrors	Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
FwdDgrams	Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
UnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	Number of datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Table 110. *IPv6 Statistics (continued)*

Statistic	Description
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their `Don't Fragment` flag was set.
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
RcvdMCastPkt	The number of multicast packets received by the interface.
SentMcastPkts	The number of multicast packets transmitted by the interface.
TruncatedPkts	The number of input datagrams discarded because datagram frame didn't carry enough data.
RcvdRedirects	The number of Redirect messages received by the interface.
SentRedirects	The number of Redirect messages sent.

The following table describes the IPv6 ICMP statistics.

Table 111. *ICMP Statistics*

Statistic	Description
Received	
ICMPPkts	Number of ICMP messages which the entity (the switch) received.
ICMPErrPkt	Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
DestUnreach	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
PktTooBigMsg	The number of ICMP Packet Too Big messages received by the interface.
ICMPEchoReq	Number of ICMP Echo (request) messages received.
ICMPEchoReps	Number of ICMP Echo Reply messages received.
RouterSols	Number of Router Solicitation messages received by the switch.
RouterAdv	Number of Router Advertisements received by the switch.
NeighSols	Number of Neighbor Solicitations received by the switch.
NeighAdv	Number of Neighbor Advertisements received by the switch.

Table 111. *ICMP Statistics*

Statistic	Description
Redirects	Number of ICMP Redirect messages received.
AdminProhib	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPBadCode	The number of ICMP Parameter Problem messages received by the interface.
Sent	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

The following table describes the UDP statistics.

Table 112. *UDP Statistics*

Statistic	Description
Received	
UDPDgrams	Number of UDP datagrams received by the switch.
UDPNoPorts	Number of received UDP datagrams for which there was no application at the destination port.
UDPErrPkts	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Sent	
UDPDgrams	Number of UDP datagrams sent from this entity (the switch).

IPv4 Route Statistics

The following command displays IPv4 route statistics:

`show ip route counters`

Command mode: All

```
Route statistics:
Current total outstanding routes     :            2
Highest number ever recorded         :            2
Current static routes                :            0
Current RIP routes                   :            0
Current OSPF routes                  :            0
Current BGP routes                   :            0
Maximum supported routes             :        15872

ECMP statistics (active in ASIC):
Maximum number of ECMP routes        :        15483
Maximum number of static ECMP routes :          128
Number of routes with ECMP paths     :            0
```

The following table describes the IPv4 route statistics.

Table 113. *IPv4 Route Statistics*

Statistics	Description
Current total outstanding routes	Total number of outstanding routes in the route table.
Highest number ever recorded	Highest number of routes ever recorded in the route table.
Current static routes	Total number of static routes in the route table.
Current RIP routes	Total number of RIP routes in the route table.
Current OSPF routes	Total number of OSPF routes in the route table.
Current BGP routes	Total number of BGP routes in the route table.
Maximum supported routes	Maximum number of routes that are supported.
Maximum number of ECMP routes	Maximum number of ECMP routes that are supported.
Maximum number of static ECMP routes	Maximum number of static ECMP routes that are supported.
Number of routes with ECMP paths	Current number of routes that contain ECMP paths.

Use the following command to clear all IPv4 route statistics:

`clear ip route counters`

Command mode: Privileged EXEC

IPv6 Route Statistics

The following command displays IPv6 route statistics:

`show ipv6 route counters`

Command mode: All

```
IPV6 Route statistics:
ipv6RoutesCur:               4  ipv6RoutesHighWater:         6
ipv6RoutesMax:            1156

ECMP statistics:
---------------
Maximum number of ECMP routes        :          600
Max ECMP paths allowed for one route :            5
Number of routes with ECMP paths     :            0
```

The following table describes the IPv6 route statistics.

Table 114. *IPv6 Route Statistics*

Statistics	Description
ipv6RoutesCur	Total number of outstanding routes in the route table.
ipv6RoutesHighWater	Highest number of routes ever recorded in the route table.
ipv6RoutesMax	Maximum number of routes that are supported.
Maximum number of ECMP routes	Maximum number of ECMP routes supported.
Max ECMP paths allowed for one route	Maximum number of ECMP paths supported for each route.
Number of routes with ECMP paths	Current number of routes that contain ECMP paths.

Use the following command to clear all IPv6 route statistics:

`clear ipv6 route counters`

Command mode: Privileged EXEC

ARP statistics

The following command displays Address Resolution Protocol statistics.

`show [ip] arp counters`

Command mode: All

```
Mgmt ARP statistics:
arpEntriesCur:             1  arpEntriesHighWater:          2

Data ARP statistics:
arpEntriesCur:             1  arpEntriesHighWater:          1
arpEntriesMax:         16383
```

The following table describes the ARP statistics.

Table 115. *ARP Statistics*

Statistic	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

The following command displays Dynamic ARP Inspection statistics.

`show ip arp inspection statistics [vlan` *<VLAN ID (1-4094)>*`]`

Command mode: All

```
Vlan  Forwarded  Dropped
----  ---------  -------
   2        100      200
```

DNS Statistics

The following command displays Domain Name System statistics.

`show ip dns counters`

Command mode: All

```
DNS statistics:
dnsInRequests:            0
dnsOutRequests:           0
dnsBadRequests:           0
```

The following table describes the DNS statistics.

Table 116. *DNS Statistics*

Statistics	Description
dnsInRequests	The total number of DNS response packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

ICMP Statistics

The following command displays ICMP statistics:

`show ip icmp counters`

Command mode: All

```
ICMP statistics:
icmpInMsgs:             245802   icmpInErrors:              1393
icmpInDestUnreachs:         41   icmpInTimeExcds:              0
icmpInParmProbs:             0   icmpInSrcQuenchs:             0
icmpInRedirects:             0   icmpInEchos:                 18
icmpInEchoReps:         244350   icmpInTimestamps:             0
icmpInTimestampReps:         0   icmpInAddrMasks:              0
icmpInAddrMaskReps:          0   icmpOutMsgs:             253810
icmpOutErrors:               0   icmpOutDestUnreachs:         15
icmpOutTimeExcds:            0   icmpOutParmProbs:             0
icmpOutSrcQuenchs:           0   icmpOutRedirects:             0
icmpOutEchos:           253777   icmpOutEchoReps:             18
icmpOutTimestamps:           0   icmpOutTimestampReps:         0
icmpOutAddrMasks:            0   icmpOutAddrMaskReps:          0
```

The following table describes the ICMP statistics.

Table 117. *ICMP Statistics*

Statistic	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by `icmpInErrors`.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.

Table 117. *ICMP Statistics*

Statistic	Description
icmpInTimestampReps	The number of ICMP Timestamp `Reply` messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by `icmpOutErrors`.
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp `Reply` messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

TCP Statistics

The following command displays TCP statistics:

`show ip tcp counters`

Command mode: All

```
TCP statistics:
tcpRtoAlgorithm:         4   tcpRtoMin:               0
tcpRtoMax:          240000   tcpMaxConn:            512
tcpActiveOpens:     252214   tcpPassiveOpens:         7
tcpAttemptFails:       528   tcpEstabResets:          4
tcpInSegs:          756401   tcpOutSegs:         756655
tcpRetransSegs:          0   tcpInErrs:               0
tcpCurrEstab:            0   tcpCurConn:              3
tcpOutRsts:            417
```

The following table describes the TCP statistics.

Table 118. *TCP Statistics*

Statistic	Description
tcpRtoAlgorithm	The algorithm used to determine the `timeout` value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Table 118. *TCP Statistics (continued)*

Statistic	Description
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP `checksums`).
tcpCurrEstab	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

UDP Statistics

The following command displays UDP statistics:

`show ip udp counters`

Command mode: All

```
UDP statistics:
udpInDatagrams:        54   udpOutDatagrams:        43
udpInErrors:            0   udpNoPorts:        1578077
```

The following table describes the UDP statistics.

Table 119. *UDP Statistics*

Statistic	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

IGMP Statistics

The following command displays statistics about the use of the IGMP Multicast Groups:

`show ip igmp counters`

Command mode: All

```
IGMP vlan 2 statistics:
-------------------------------------------------------------------------
rxIgmpValidPkts:                0   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:               0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:  0   rxIgmpDiscardPkts:                0
rxIgmpLeaves:                   0   rxIgmpReports:                    0
txIgmpReports:                  0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                   0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0   rxIgmpV3FilterChangeRecords:      0
txIgmpGenQueries:               0   rxPimHellos:                      0
```

The following command displays statistics about the use of the IGMP Multicast Groups for a specific VLAN:

`show ip igmp vlan` *<VLAN ID (1-4094)>* **`counter`**

Command mode: All

```
IGMP vlan 147 statistics:
-------------------------------------------------------------------------
rxIgmpValidPkts:                0   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:               0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:  0   rxIgmpDiscardPkts:                0
rxIgmpLeaves:                   0   rxIgmpReports:                    0
txIgmpReports:                  0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                   0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0   rxIgmpV3FilterChangeRecords:      0
txIgmpGenQueries:               0   rxPimHellos:                      0
```

The following table describes the IGMP statistics.

Table 120. *IGMP Statistics*

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received

Table 120. *IGMP Statistics (continued)*

Statistic	Description
rxIgmpDiscardPkts	Total number of IGMP packets discarded
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received
txIgmpGenQueries	Total number of General Membership Query packets transmitted
rxPimHellos	Total number of PIM hellos received

MLD Statistics

The following table describes the commands used to view MLD statistics.

Table 121. *MLD Statistics Commands*

Command Syntax and Usage
show ipv6 mld counters Displays MLD statistics. See page 272 for sample output. **Command mode:** All
show ipv6 mld groups counters Displays total number of MLD entries. **Command mode:** All
show ipv6 mld interface counters Displays total number of MLD entries. **Command mode:** All
show ipv6 mld interface *<1-126>* **counters** Displays total number of MLD entries on the interface. **Command mode:** All
clear ipv6 mld counters Clears MLD counters. **Command mode:** Privileged EXEC

MLD Global Statistics

The following command displays MLD global statistics for all MLD packets received on all interfaces:

`show ipv6 mld counters`

Command mode: All

```
MLD global statistics:
----------------------
Total L3 IPv6 (S, G, V) entries:  2
Total MLD groups:                 2
Bad Length:                       0
Bad Checksum:                     0
Bad Receive If:                   0
Receive non-local:                0
Invalid Packets:                  4

MLD packet statistics for interfaces:

MLD interface packet statistics for interface 1:
MLD msg type           Received                 Sent              xErrors
-------------- ---------------- -------------------- --------------------
General Query                 0                 1067                    0
MAS Query                     0                    0                    0
MASSQ Query                   0                    0                    0
MLDv1 Report                  0                    0                    0
MLDv1 Done                    0                    0                    0
MLDv2 Report               1069                 1084                    0
INC CSRs(v2)                  1                    0                    0
EXC CSRs(v2)               2134                 1093                    0
TO_INC FMCRs(v2)              1                    0                    0
TO_EXC FMCRs(v2)              0                   15                    0
ALLOW SLCRs(v2)               0                    0                    0
BLOCK SLCRs(v2)               0                    0                    0

MLD interface packet statistics for interface 2:

MLD msg type           Received                 Sent              xErrors
-------------- ---------------- -------------------- --------------------

MLD interface packet statistics for interface 3:

MLD msg type           Received                 Sent              xErrors
-------------- ---------------- -------------------- --------------------
General Query                 0                 2467                    0
MAS Query                     0                    0                    0
MASSQ Query                   0                    0                    0
MLDv1 Report                  0                    0                    0
MLDv1 Done                    0                    0                    0
MLDv2 Report                  2                 2472                    0
INC CSRs(v2)                  1                    0                    0
EXC CSRs(v2)                  0                 2476                    0
TO_INC FMCRs(v2)              0                    0                    0
TO_EXC FMCRs(v2)              0                    8                    0
ALLOW SLCRs(v2)               0                    0                    0
BLOCK SLCRs(v2)               1                    0                    0
```

The following table describes the fields in the MLD global statistics output.

Table 122. *MLD Global Statistics*

Statistic	Description
Bad Length	Number of messages received with length errors.
Bad Checksum	Number of messages received with an invalid IP checksum.
Bad Receive If	Number of messages received on an interface not enabled for MLD.
Receive non-local	Number of messages received from non-local senders.
Invalid packets	Number of rejected packets.
General Query (v1/v2)	Number of general query packets.
MAS Query(v1/v2)	Number of multicast address specific query packets.
MASSQ Query(v2)	Number of multicast address and source specific query packets.
Listener Report(v1)	Number of packets sent by a multicast listener in response to MLDv1 query.
Listener Done(v1/v2)	Number of packets sent by a host when it wants to stop receiving multicast traffic.
Listener Report(v2)	Number of packets sent by a multicast listener in response to MLDv2 query.
MLDv2 INC mode CSRs	Number of current state records with include filter mode.
MLDv2 EXC mode CSRs	Number of current state records with exclude filter mode.
MLDv2 TO_INC FMCRs	Number of filter mode change records for which the filter mode has changed to include mode.
MLDv2 TO_EXC FMCRs	Number of filter mode change records for which the filter mode has changed to exclude mode.
MLDv2 ALLOW SLCRs	Number of source list change records for which the specified sources from where the data is to be received has changed.
MLDv2 BLOCK SLCRs	Number of source list change records for which the specified sources from where the data is to be received is to be blocked.

OSPF Statistics

The following commands display OSPF statistics:

Table 123. *OSPF Statistics Commands*

Command Syntax and Usage
show ip ospf counters Displays global OSPF statistics. See page 275 for sample output. **Command mode:** All
show ip ospf area [*<0-19>***] counters** Displays OSPF statistics for all areas or a specified area. **Command mode:** All
show ip ospf interface [*<interface number>***|port** *<port alias or number>***] counters** Displays OSPF statistics for all interfaces or a specified interface. **Command mode:** All
clear ip ospf counters Clears OSPF statistics. **Command mode:** Privileged EXEC

OSPF Global Statistics

The following command displays statistics about OSPF packets received on all OSPF areas and interfaces:

`show ip ospf counters`

Command mode: All

```
OSPF stats
----------
Rx/Tx Stats:            Rx            Tx
                     --------      --------
  Pkts                    0             0
  hello                  23           518
  database                4            12
  ls requests             3             1
  ls acks                 7             7
  ls updates              9             7

Nbr change stats:                 Intf change Stats:
  hello                   2            hello              4
  start                   0            down               2
  n2way                   2            loop               0
  adjoint ok              2            unloop             0
  negotiation done        2            wait timer         2
  exchange done           2            backup             0
  bad requests            0            nbr change         5
  bad sequence            0
  loading done            2
  n1way                   0
  rst_ad                  0
  down                    1

Timers kickoff
  hello                 514
  retransmit           1028
  lsa lock                0
  lsa ack                 0
  dbage                   0
  summary                 0
  ase export              0
```

The following table describes the OSPF general statistics.

Table 124. *OSPF General Statistics*

Statistic	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.

Table 124. *OSPF General Statistics (continued)*

Statistic	Description
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Nbr Change Stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of `HelloInterval` seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.

Table 124. *OSPF General Statistics (continued)*

Statistic	Description
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	The sum total number of Database Description packets which have been received that either: • Has an unexpected DD sequence number • Unexpectedly has the init bit set • Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.
Intf Change Stats:	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

Table 124. *OSPF General Statistics (continued)*

Statistic	Description
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA `Ack` timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (`Dbage`) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

OSPFv3 Statistics

The following commands display OSPFv3 statistics:

Table 125. *OSPFv3 Statistics Commands*

Command Syntax and Usage
show ipv6 ospf counters Displays OSPFv3 statistics. See page 280 for sample output. **Command mode:** All
show ipv6 ospf area [<*area index (0-2)*>**] counters** Displays OSPFv3 statistics for all areas or a specified area. **Command mode:** All
show ipv6 ospf interface [<*interface number*>**] counters** Displays OSPFv3 statistics for all interfaces or a specified interface. **Command mode:** All
clear ipv6 ospf counters Clears OSPFv3 statistics. **Command mode:** Privileged EXEC

OSPFv3 Global Statistics

The following command displays statistics about OSPFv3 packets received on all OSPFv3 areas and interfaces:

`show ipv6 ospf counters`

Command mode: All

```
OSPFv3 stats
----------
Rx/Tx/Disd Stats:          Rx            Tx         Discarded
                        --------      --------      ---------
       Pkts               9695          95933             0
       hello              9097           8994             0
       database             39             51             6
       ls requests          16              8             0
       ls acks             172            360             0
       ls updates          371            180             0

Errors
  rx on pasv intf           0
  rx but ospf off           0
  rx on intf not up         0
  rx version mismatch       0
  rx rtr id is zero         0
  rx with our rtr id        0
  instance id mismatch      0
  area mismatch             0
  dest addr mismatch        0
  bad checksum              0
  no associated nbr         0
  bad packet type           0
  hello mismatch            0
  options mismatch          0
  dead mismatch             0
  bad nbma/ptomp nbr        0

Nbr change stats:                Intf change Stats:
  down                   0           down               5
  attempt                0           loop               0
  init                   1           waiting            6
  n2way                  1           ptop               0
  exstart                1           dr                 4
  exchange done          1           backup             6
  loading done           1           dr other           0
  full                   1           all events        33
  all events             6

Timers kickoff
  hello                  8988
  wait                   6
  poll                   0
  nbr probe              0
```

The OSPFv3 General Statistics contain the sum total of all OSPFv3 packets received on all OSPFv3 areas and interfaces.

The following table describes the OSPFv3 general statistics.

Table 126. *OSPFv3 General Statistics*

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
Discarded Pkts	The sum total of all OSPFv3 packets discarded.
Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.
Discarded hello	The sum total of all Hello packets discarded, including packets for which no associated interface has been found.
Rx database	The sum total of all Database Description packets received on all OSPFv3 interfaces.
Tx database	The sum total of all Database Description packets transmitted on all OSPFv3 interfaces.
Discarded database	The sum total of all Database Description packets discarded.
Rx ls requests	The sum total of all Link State Request packets received on all OSPFv3 interfaces.
Tx ls requests	The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces.
Discarded ls requests	The sum total of all Link State Request packets discarded.
Rx ls acks	The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces.
Tx ls acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces.
Discarded ls acks	The sum total of all Link State Acknowledgement packets discarded.
Rx ls updates	The sum total of all Link State Update packets received on all OSPFv3 interfaces.

Table 126. *OSPFv3 General Statistics (continued)*

Statistics	Description
Tx ls updates	The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces.
Discarded ls updates	The sum total of all Link State Update packets discarded.
Nbr Change Stats:	
down	The total number of Neighboring routers down (in the initial state of a neighbor conversation) across all OSPFv3 interfaces.
attempt	The total number of transitions into attempt state of neighboring routers across allOSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces
exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.
Intf Change Stats:	
down	The total number of transitions into down state of all OSPFv3 interfaces.
loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.

Table 126. *OSPFv3 General Statistics (continued)*

Statistics	Description
backup	The total number of transitions into backup state of all OSPFv3 interfaces.
all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
Timers Kickoff:	
hello	The total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OSPFv3 interfaces.
wait	The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces.
poll	The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces.
nbr probe	The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces.
Number of LSAs:	
originated	The number of LSAs originated by this router.
rcvd newer originations	The number of LSAs received that have been determined to be newer originations.

VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the G8272 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the protocol statistics for VRRP. The following command displays VRRP statistics:

`show ip vrrp counters`

Command mode: All

```
VRRP statistics:
vrrpInAdvers:             0   vrrpBadAdvers:                  0
vrrpOutAdvers:            0   vrrpOutGratuitousARPs:          0
vrrpBadVersion:           0   vrrpBadVrid:                    0
vrrpBadAddress:           0   vrrpBadData:                    0
vrrpBadPassword:          0   vrrpBadInterval:                0
```

The following table describes the VRRP statistics.

Table 127. *VRRP Statistics*

Statistics	Description
vrrpInAdvers	The total number of valid VRRP advertisements that have been received.
vrrpBadAdvers	The total number of VRRP advertisements received that were dropped.
vrrpOutAdvers	The total number of VRRP advertisements that have been sent.
vrrpBadVersion	The total number of VRRP advertisements received that had a bad version number.
vrrpOut GratuitousARPs	The total number of VRRP gratuitous ARPs that have been sent.
vrrpBadVrid	The total number of VRRP advertisements received that had a bad virtual router ID.
vrrpBadAddress	The total number of VRRP advertisements received that had a bad address.
vrrpBadData	The total number of VRRP advertisements received that had bad data.
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.

PIM Statistics

The following command displays Protocol Independent Multicast (PIM) statistics:

`show ip pim counters`

Command mode: All

```
Hello Tx/Rx      : 2595/2596
Join/Prune Tx/Rx : 0/0
Assert Tx/Rx     : 0/0
Register Tx/Rx   : 0/0
Null-Reg Tx/Rx   : 0/0
RegStop Tx/Rx    : 0/0
CandRPAdv Tx/Rx  : 973/0
BSR Tx/Rx        : 0/1298
Graft Tx/Rx      : 0/0
Graft Ack Tx/Rx  : 0/0
Mcast data Tx/Rx : 0/0
MDP drop Tx/Rx   : 0/0
CTL drop Tx/Rx   : 0/0
Bad pkts         : 0
```

The following table describes the PIM statistics.

Table 128. *PIM Statistics*

Statistics	Description
Hello Tx/Rx	Number of Hello messages transmitted or received
Join/Prune Tx/Rx	Number of Join/Prune messages transmitted or received
Assert Tx/Rx	Number of Assert messages transmitted or received
Register Tx/Rx	Number of Register messages transmitted or received
Null-Reg Tx/Rx	Number of NULL-register messages received
RegStop Tx/Rx	Number of Register Stop messages transmitted or received
CandRPAdv Tx/Rx	Number of Candidate RP Advertisements transmitted or received
BSR Tx/Rx	Number of Bootstrap Router (BSR) messages transmitted or received
Graft Tx/Rx	Number of Graft messages transmitted or received
Graft Ack Tx/Rx	Number of Graft Acknowledgements transmitted or received
Mcast data Tx/Rx	Number of multicast datagrams transmitted or received
MDP drop Tx/Rx	Number of Multicast data packet Tx/Rx dropped
CTL drop Tx/Rx	Number of PIM control packet Tx/Rx dropped
Bad pkts	Number of bad PIM packets received

Routing Information Protocol Statistics

The following command displays RIP statistics:

`show ip rip counters`

Command mode: All

```
RIP ALL STATS INFORMATION:
        RIP packets received  = 12
        RIP packets sent      = 75
        RIP request received  = 0
        RIP response recevied = 12
        RIP request sent      = 3
        RIP reponse sent      = 72
        RIP route timeout     = 0
        RIP bad size packet received   = 0
        RIP bad version received       = 0
        RIP bad zeros received         = 0
        RIP bad src port received      = 0
        RIP bad src IP received        = 0
        RIP packets from self received = 0
```

DHCP Statistics

The following commands display DHCP statistics:

Table 129. *DHCP Statistics Options*

Command Syntax and Usage
show ip dhcp snooping counters Displays DHCP Snooping statistics. **Command mode:** All
clear ip dhcp snooping counters Clears DHCP Snooping statistics. **Command mode:** Privileged EXEC

DHCP Snooping Statistics

The following command displays DHCP Snooping statistics:

show ip dhcp snooping counters

Command mode: All

```
DHCP Snooping statistics:
Received Request packets               2
Received Reply packets                 2
Recevied Invalid packets               0
Dropped packets out of rate            0
Dropped packets other reason           0
```

DHCP Snooping Statistics count all DHCP packets processed by DHCP snooping.

OpenFlow Statistics

The following commands display OpenFlow statistics:

Table 130. *OpenFlow Statistics Commands*

Command Syntax and Usage
show openflow statistics Displays OpenFlow traffic statistics for each OpenFlow instance. **Command mode:** All
show openflow instance *<1-2>* **statistics** Displays OpenFlow traffic statistics for the specified instance ID. **Command mode:** All
clear openflow statistics Clears OpenFlow data for all instances. **Command mode:** Privileged EXEC
clear openflow instance *<1-2>* **statistics** Clears OpenFlow data for the specified instance ID. **Command mode:** Privileged EXEC

Use the following command to display OpenFlow traffic statistics for each OpenFlow instance:

show openflow statistics

Command mode: All

In OpenFlow 1.0:

```
Openflow instance 1 is currently disabled
-----------------------------------------------------------
Openflow statistics for instance 2
Flow Count
        Basic Flows:     3
           (ACL Based: 3, Unicast FDB Based: 0, Multicast FDB Based: 0)
        Emergency Flows: 0
           (ACL Based: 0, Unicast FDB Based: 0, Multicast FDB Based: 0)

Buffering Count:
        Openflow Packets Buffered  : 0
        Openflow Packets Timed out : 0
        Openflow Packets Retrieved : 0
        Openflow Packets Retrieve attempts : 0
Message Count
Hello-Sent: 1                   Hello-Received: 1
Echo-Request-Sent: 31           Echo-Request-Received: 60
Echo-Reply-Sent: 60             Echo-Reply-Received: 31
Vendor: 0
```

```
Vendor Flow-Mod:
        Add: 0
        Modify: 0
        Modify-Strict: 0
        Delete: 0
        Delete-Strict: 0
Feature-Request: 1              Feature-Reply: 1
Get-Config-Request: 0           Get-Config-Reply: 0
Set-Config: 1
Packet-In
        No-Match: 0
        Action: 0
        Action Mirror: 0
Flow-Removed:
        Idle-Timeout: 0
        Hard-Timeout: 0
        Delete: 0
Vendor-Flow-Removed:
        Idle-Timeout: 0
        Hard-Timeout: 0
        Delete: 0
Port-Status:
        Add: 0
        Delete: 0
        Modify: 0
Packet-Out: 1088
Flow-Mod:
        Add: 3
        Modify: 0
        Modify-Strict: 0
        Delete: 0
        Delete-Strict: 1
Port-Mod: 0
Statistics-Request:
        Desc: 1
        Flow: 15
        Aggregate: 0
        Table: 0
        Port: 15
        Vendor: 0
                stats: 0
                stats-strict: 0
Statistics-Reply:
        Desc: 1
        Flow: 15
        Aggregate: 0
        Table: 0
        Port: 15
        Vendor: 0
                stats: 0
                stats-strict: 0
Barrier-Request: 2
Barrier-Reply: 2
Error Messages
Hello Failed Sent:
        Incompatible: 0
Hello Failed Recv:
        Incompatible: 0
```

```
Bad Request:
        Bad-Version: 0
        Bad-Type: 0
        Bad-Stat: 0
        Bad-Vendor: 0
        Bad-Subtype: 0
        Bad-Len: 0
        Buffer-Empty: 0
        Buffer-Unknown: 0
Bad Action:
        Bad-Type: 0
        Bad-Len: 0
        Bad-Out-Port: 0
        Bad-Argument: 0
        Too-many: 0
Flow-Mod-Failed:
        All-Table-Full: 0
        Overlap: 0
        Permission-Error: 0
        Emergency-Timeout: 0
        Bad-Command: 0
        Unsupported: 0
Port-Mod-Failed:
        Bad-Port: 0
        Bad-hw-addr: 0
```

In Openflow 1.3:

```
Openflow statistics for instance 1
Flow Count
        Static Flows: 0
                ACL Based: 0
                Mpls PUSH based: 0
                Mpls POP based: 0
        Dynamic Flows: 2
                ACL Based: 2
                Unicast FDB Based: 0
                Multicast FDB Based: 0
                Mpls PUSH based: 0
                Mpls POP based: 0
Group Count: 0

Buffering Count:
        Openflow Packets Buffered  : 0
        Openflow Packets Timed out : 0
        Openflow Packets Retrieved : 0
        Openflow Packets Retrieve attempts : 0
Message Count
Hello-Sent: 3                   Hello-Received: 3
Echo-Request-Sent: 12003        Echo-Request-Received: 23857
Echo-Reply-Sent: 23857          Echo-Reply-Received: 12002
Feature-Request: 3              Feature-Reply: 3
Get-Config-Request: 0           Get-Config-Reply: 0
Set-Config: 3
Packet-In
        No-Match: 0
        Action: 0
```

```
Flow-Removed:
        Idle-Timeout: 0
        Hard-Timeout: 0
        Delete: 0
        Group-Delete: 0
Port-Status:
        Add: 1
        Delete: 0
        Modify: 3
Packet-Out: 33054
Flow-Mod:
        Add: 6
        Modify: 0
        Modify-Strict: 0
        Delete: 0
        Delete-Strict: 0
Group-Mod:
        Add: 0
        Modify: 0
        Delete: 0
Port-Mod: 0
Multipart-Request:
        Switch description: 6
        Individual flow statistics: 5993
        Aggregate flow statistics: 0
        Flow table statistics: 0
        Port statistics: 5993
        Group counter statistics: 0
        Group description: 0
        Group features: 0
        Port description: 3
Multipart-Reply:
        Switch description: 6
        Individual flow statistics: 5993
        Aggregate flow statistics: 0
        Flow table statistics: 0
        Port statistics: 5993
        Group counter statistics: 0
        Group description: 0
        Group features: 0
        Port description: 3

Barrier-Request: 3
Barrier-Reply: 3
Error Messages
Hello Failed Sent:
        Incompatible: 0
Hello Failed Recv:
        Incompatible: 0
Bad Request:
        Bad-Version: 0
        Bad-Type: 0
        Bad-Multipart: 0
        Permission-error: 0
        Bad-Len: 0
        Buffer-Empty: 0
        Buffer-Unknown: 0
        Bad-Table-ID: 0
        Bad-Port: 0
        Bad-Packet: 0
        Multipart-Buffer-Overflow: 0
```

```
Bad Action:
        Bad-Type: 0
        Bad-Len: 0
        Bad-Out-Port: 0
        Bad-Argument: 0
        Permission-Error: 0
        Too-many: 0
        Bad-Out-Group: 0
        Match-Inconsistent: 0
        Unsupported-Order: 0
        Bad-Set-Type: 0
        Bad-Set-Len: 0
        Bad-Set-Argument: 0
Bad Instruction:
        Unknown-Instruction: 0
        Unsupport-Instruction: 0
        Bad-Len: 0
        Permission-Error: 0
Bad Match:
        Bad-Type: 0
        Bad-Len: 0
        Bad-MAC-Addr-Mask: 0
        Bad-IP-Addr-Mask: 0
        Bad-Wildcards: 0
        Bad-Field: 0
        Bad-Value: 0
        Bad-Mask: 0
        Bad-Prerequisites: 0
        Duplicated-Field: 0
Flow-Mod-Failed:
        Unknown: 0
        Table-Full: 0
        Bad-Table-ID: 0
        Overlap: 0
        Permission-Error: 0
        Bad-Timeout: 0
        Bad-Command: 0
        Bad-Flags: 0
Group-Mod-Failed:
        Group-Exists: 0
        Invalid-Group: 0
        Weight-Unsupported: 0
        Out-of-Groups: 0
        Out-of-Buckets: 0
        Chaining-Unsupported: 0
        Watch-Unsupported: 0
        Loop: 0
        Unknown-Group: 0
        Chained-Group: 0
        Bad-Type: 0
        Bad-Command: 0
        Bad-Bucket: 0
        Bad-Watch: 0
        Permission-Error: 0
Port-Mod-Failed:
        Bad-Port: 0
        Bad-hw-addr: 0
        Bad-Config: 0
        Bad-Advertise: 0
        Permission-Error: 0
Switch-Config-Failed:
        Bad-Flags: 0
        Permission-Error: 0
Openflow instance 2 is currently disabled
```

The following table describes the OpenFlow statistics.

Table 131. *OpenFlow Statistics*

Parameter	Description
Flow Count	
Basic Flows	Count of flows stored in the basic flow table, sorted by type: ACL, unicast FDB and multicast FDB.
Emergency Flows	Count of flows stored in the emergency flow table, sorted by type: ACL, unicast FDB and multicast FDB.
Static Flows	Count of flows stored in the static flow table, sorted by type: ACL, unicast FDB, multicast FDB, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
Dynamic Flows	Count of flows stored in the dynamic flow table, sorted by type: ACL, unicast FDB, multicast FDB, MPLS push and MPLS pop. Available only in OpenFlow 1.3.
Group Count	Count of installed groups.
Buffering Count	
Openflow Packets Buffered	Count of packets buffered.
Openflow Packets Timed out	Count of buffered packets dropped due to time out.
Openflow Packets Retrieved	Count of packets retrieved.
Openflow Packets Retrieve attempts	Count of attempts made to retrieve the buffer.
Message Count	Count of messages exchanged between the Controller and the switch.
Hello-Sent	Count of `Hello` messages sent from the switch to the Controller.
Hello-Received	Count of `Hello` messages received by the switch from the Controller.
Echo-Request-Sent	Count of `Echo Request` messages sent from the switch to the Controller.
Echo-Request-Received	Count of `Echo Request` messages received by the switch from the Controller.
Echo-Reply-Sent	Count of `Echo Reply` messages sent by the switch to the Controller.
Echo-Reply-Received	Count of `Echo Reply` messages received by the switch from the Controller.

Table 131. *OpenFlow Statistics*

Parameter	Description
Vendor	Count of `Vendor` messages received by the switch from the Controller. Available only in OpenFlow 1.0.
Vendor Flow-Mod	Available only in OpenFlow 1.0.
Add	Count of vendor-defined `add flow_mod` messages received by the switch. Available only in OpenFlow 1.0.
Modify	Count of vendor-defined `modify flow_mod` messages received by the switch. Available only in OpenFlow 1.0.
Modify-Strict	Count of vendor-defined `modify_strict flow_mod` messages received by the switch. Available only in OpenFlow 1.0.
Delete	Count of vendor-defined `delete flow_mod` messages received by the switch. Available only in OpenFlow 1.0.
Delete-Strict	Count of vendor-defined `delete-strict flow_mod` messages received by the switch. Available only in OpenFlow 1.0.
Feature-Request	Count of `Feature Request` messages received from the Controller by the switch.
Feature-Reply	Count of `Feature Reply` messages sent from the switch to the Controller.
Get-Config-Request	Count of `Get Config Request` messages received from the Controller by the switch.
Get-Config-Reply	Count of `Get Config Reply` messages sent from the switch to the Controller.
Set-Config	Count of `Set Config` messages received from the Controller by the switch.
Packet-In	
No-Match	Count of `Packet-In` messages sent to the Controller due to no matching flows.
Action	Count of `Packet-In` messages sent to the Controller due to action explicitly asking to forward to the Controller.
Action Mirror	Count of NEC specific `Packet-In` messages sent to the Controller due to action explicitly asking to forward to the Controller. Available only in OpenFlow 1.0.

Table 131. *OpenFlow Statistics*

Parameter	Description
Flow-Removed	
Idle-Timeout	Count of flow entries removed due to idle-timeout expiration.
Hard-Timeout	Count of flow entries removed due to hard-timeout expiration.
Delete	Count of flow entries removed due to explicit deletion.
Group-Delete	Count of flow entries removed due to deletion of associated group. Available only in OpenFlow 1.3.
Vendor-Flow-Removed	Available only in OpenFlow 1.0.
Idle-Timeout	Count of vendor-defined flow entries removed due to idle-timeout expiration. Available only in OpenFlow 1.0.
Hard-Timeout	Count of vendor-defined flow entries removed due to hard-timeout expiration. Available only in OpenFlow 1.0.
Delete	Count of vendor-defined flow entries removed due to explicit deletion. Available only in OpenFlow 1.0.
Port-Status	
Add	Count of `port-status` messages sent triggered by adding a port to OpenFlow.
Delete	Count of `port-status` messages sent triggered by removing a port from OpenFlow.
Modify	Count of `port-status` messages sent triggered by a modification of a port belonging to OpenFlow (for example, up/down status).
Packet-Out	Count of `packet-out` messages received from the Controller.
Flow-Mod	
Add	Count of `add flow_mod` messages received by the switch.
Modify	Count of `modify flow_mod` messages received by the switch.
Modify-Strict	Count of `modify_strict flow_mod` messages received by the switch.
Delete	Count of `delete flow_mod` messages received by the switch.
Delete-Strict	Count of `delete-strict flow_mod` messages received by the switch.

Table 131. *OpenFlow Statistics*

Parameter	Description
Group-Mod	Available only in OpenFlow 1.3
Add	Count of Group Add messages received from Controller. Available only in OpenFlow 1.3.
Modify	Count of Group Modify messages received from Controller. Available only in OpenFlow 1.3.
Delete	Count of Group Delete messages received from Controller. Available only in OpenFlow 1.3.
Port-Mod	Count of `port_mod` messages received by the switch from the Controller.
Statistics-Request	Available only in OpenFlow 1.0.
Desc	Count of Description statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Vendor	Available only in OpenFlow 1.0.
stats	Count of Vendor statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests received from the Controller by the switch. Available only in OpenFlow 1.0.
Statistics-Reply	Available only in OpenFlow 1.0.
Desc	Count of Description statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
Flow	Count of Flow statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
Aggregate	Count of Aggregate statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
Table	Count of Table statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
Port	Count of Port statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.

Table 131. *OpenFlow Statistics*

Parameter	Description
Vendor	Available only in OpenFlow 1.0.
stats	Count of Vendor statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
stats-strict	Count of Vendor strict statistics requests sent to the Controller by the switch. Available only in OpenFlow 1.0.
Multipart-Request	Available only in OpenFlow 1.3
Switch description	Count of Switch Description requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Individual flow statistics	Count of Individual Flow statistics requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Group counter statistics	Count of Group statistics requests received from the Controller. Available only in OpenFlow 1.3.
Group description	Count of Group description requests received from the Controller. Available only in OpenFlow 1.3.
Group features	Count of Group features requests received from the Controller. Available only in OpenFlow 1.3.
Port description	Count of Port descriptions requests received from the Controller by the switch. Available only in OpenFlow 1.3.
Multipart-Reply	Available only in OpenFlow 1.3
Switch description	Count of Switch Description replies sent to the Controller by the switch. Available only in OpenFlow 1.3.
Individual flow statistics	Count of Individual Flow statistics replies sent to the Controller by the switch. Available only in OpenFlow 1.3.
Aggregate flow statistics	Count of Aggregate statistics replies sent to the Controller by the switch. Available only in OpenFlow 1.3.
Flow table statistics	Count of Table statistics replies sent to the Controller by the switch. Available only in OpenFlow 1.3.
Port statistics	Count of Port statistics replies sent to the Controller by the switch. Available only in OpenFlow 1.3.

Table 131. *OpenFlow Statistics*

Parameter	Description
Group counter statistics	Count of Group statistics replies sent to the Controller. Available only in OpenFlow 1.3.
Group description	Count of Group description replies sent to the Controller. Available only in OpenFlow 1.3.
Group features	Count of Group features replies sent to the Controller. Available only in OpenFlow 1.3.
Port description	Count of Port description replies sent to the Controller by the switch. Available only in OpenFlow 1.3.
Barrier-Request	Count of `barrier-request` messages received from the Controller by the switch.
Barrier-Reply	Count of `barrier-reply` messages sent to the Controller by the switch.
Error Messages	Count of error messages handled - sending/receiving error messages.
Hello Failed Sent	
Incompatible	Count of error messages sent by the switch if the version in the `Hello` message is incompatible with the version of the Controller.
Hello Failed Recv	
Incompatible	Count of error messages received by the switch if the version in the `Hello` message is incompatible with the version of the Controller.
Bad Request	
Bad-Version	Count of error messages sent due to `bad-version` in the request header.
Bad-Type	Count of error messages sent due to `bad-type` in the request header.
Bad-Stat	Count of error messages sent due to a specific statistics request that is not supported. Available only in OpenFlow 1.0.
Bad-Vendor	Count of error messages sent due to vendor-specific message that is not supported. Available only in OpenFlow 1.0.
Bad-Subtype	Count of error messages sent due to message subtype that is not supported. Available only in OpenFlow 1.0.
Bad-Multipart	Count of error messages sent due to unknown multipart request type specified in the `multipart-request` message. Available only in OpenFlow 1.3.

Table 131. *OpenFlow Statistics*

Parameter	Description
Permission-error	Count of error messages sent because the action received in the `flow-mod` message `Port-Mod-Failed` is not permitted. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong request length for type of message received in the request header.
Buffer-Empty	Count of error messages sent when the specified buffer in the request does not exist.
Buffer-Unknown	Count of error messages sent when the specified buffer in the request is unknown.
Bad-Table-ID	Count of error messages sent when the specified `table-id` in the request is invalid or the `table-id` doesn't exist. Available only in OpenFlow 1.3.
Bad-Port	Count of error messages sent due to invalid port in the `port-mod` message. Available only in OpenFlow 1.3.
Bad-Packet	Count of error messages sent when the specified packet is invalid in `packet-out`. Available only in OpenFlow 1.3.
Multipart-Buffer-Overflow	Count of error messages sent when the specified buffer in the `multi-part` request is overflowed. Available only in OpenFlow 1.3.
Bad Action	
Bad-Type	Count of error messages sent due to due to unknown action type specified in `flow_mod` message.
Bad-Len	Count of error messages sent due to wrong action length for type of message received in the `flow_mod` message.
Bad-Out-Port	Count of error message sent due to invalid port in the action field specified `flow_mod` message.
Bad-Argument	Count of error message sent due to bad action argument in `flow_mod` message that is not supported.
Permission-Error	Count of error message sent due to permission error while processing the flow_mod message received. Available only in OpenFlow 1.3.
Too-Many	Count of error message sent due to too many actions received in the `flow_mod` message that cannot be handled.
Bad-Out-Group	Count of error message sent due to inexistent group in the flow_mod message received. Available only in OpenFlow 1.3.

Table 131. *OpenFlow Statistics*

Parameter	Description
Match-Inconsistent	Count of error messages sent because the action cannot apply for this match or because there is a `set-field` missing prerequisite. Available only in OpenFlow 1.3.
Unsupported-Order	Count of error messages sent because the action order in an `apply-actions` instruction is unsupported for the action list. Available only in OpenFlow 1.3.
Bad-Set-Type	Count of error messages sent due to unsupported type in the `set-field` action. Available only in OpenFlow 1.3.
Bad-Set-Len	Count of error messages sent due to length problem in the `set-field` action. Available only in OpenFlow 1.3.
Bad-Set-Argument	Count of error messages sent due to bad argument in the `set-field` action. Available only in OpenFlow 1.3.
Bad Instruction	Available only in OpenFlow 1.3
Unknown-Instruction	Count of error messages sent due to unknown instruction in the received `flow-mod` message. Available only in OpenFlow 1.3.
Unsupport-Instruction	Count of error messages sent due to unsupported instruction in the received `flow-mod` message. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong instruction length. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the instruction. Available only in OpenFlow 1.3.
Bad Match	Available only in OpenFlow 1.3
Bad-Type	Count of error messages sent due to unsupported match type in the match. Available only in OpenFlow 1.3.
Bad-Len	Count of error messages sent due to wrong match length. Available only in OpenFlow 1.3.
Bad-MAC-Addr-Mask	Count of error messages sent due to unsupported MAC address mask in the match. Available only in OpenFlow 1.3.
Bad-IP-Addr-Mask	Count of error messages sent due to unsupported IP address mask in the match. Available only in OpenFlow 1.3.
Bad-Wildcards	Count of error messages sent due to unsupported combination of fields masked or omitted in the match. Available only in OpenFlow 1.3.

Table 131. *OpenFlow Statistics*

Parameter	Description
Bad-Field	Count of error messages sent due to unsupported field type in the match. Available only in OpenFlow 1.3.
Bad-Value	Count of error messages sent due to unsupported value in a match field. Available only in OpenFlow 1.3.
Bad-Mask	Count of error messages sent due to unsupported mask (neither a MAC address nor an IP address mask) in the match. Available only in OpenFlow 1.3.
Bad-Prerequisites	Count of error messages sent due to unfulfilled prerequisite in the match. Available only in OpenFlow 1.3.
Duplicated-Field	Count of error messages sent due to duplicated fields in the match. Available only in OpenFlow 1.3.
Flow-Mod-Failed	
All-Table-Full	Count of error messages due to table full when adding or updating `flow_mod` message. Available only in OpenFlow 1.0.
Unknown	Count of error messages sent when the error is unspecified. Available only in OpenFlow 1.3.
Table-Full	Count of error messages sent because of full table when adding or updating the `flow-mod` message. Available only in OpenFlow 1.3.
Bad-Table-ID	Count of error messages sent because the specified `table-id` in the `flow-mod` message is invalid or because the `table-id` doesn't exist. Available only in OpenFlow 1.3.
Overlap	Count of error messages sent due to an attempt to add overlapping `flow_mod` messages.
Permission-Error	Count of error messages due to permissions not available to perform action received in the `flow_mod` message `Port_Mod_Failed`.
Emergency-Timeout	Count of error messages sent due to invalid emergency-timeout in the `flow-mod` message. Available only in OpenFlow 1.0.
Bad-Timeout	Count of error messages sent when the specified idle/hard timeout in the `flow_mod` message is unsupported. Available only in OpenFlow 1.3.
Bad-Command	Count of error messages sent due to unknown command.
Unsupported	Count of error messages sent due to unsupported action list. Available only in OpenFlow 1.0.

Table 131. *OpenFlow Statistics*

Parameter	Description
Bad-Flags	Count of error messages sent when the specified flags in the `flow_mod` message are unsupported. Available only in OpenFlow 1.3.
Group-Mod-Failed	Available only in OpenFlow 1.3
Group-Exists	Count of error message sent to Controller due to already existing group. Available only in OpenFlow 1.3.
Invalid-Group	Count of error message sent to Controller due to invalid group. Available only in OpenFlow 1.3.
Weight-Unsupported	Count of error message sent to Controller due to unsupported "weight" parameter. Available only in OpenFlow 1.3.
Out-of-Groups	Count of error message sent to Controller due to full group table. Available only in OpenFlow 1.3.
Out-of-Buckets	Count of error message sent to Controller due to full bucket count per group. Available only in OpenFlow 1.3.
Chaining-Unsupported	Count of error message sent to Controller due to unsupported groups that forward to groups. Available only in OpenFlow 1.3.
Watch-Unsupported	Count of error message sent to Controller due to unsupported "watch" parameter. Available only in OpenFlow 1.3.
Loop	Count of error message sent to Controller due to unsupported checking that no loop is created while chaining groups. Available only in OpenFlow 1.3.
Unknown-Group	Count of error message sent to Controller due to unsupported group type. Available only in OpenFlow 1.3.
Chained-Group	Count of error message sent to Controller due to unsupported groups that forward to groups. Available only in OpenFlow 1.3.
Bad-Type	Count of error message sent to Controller due to wrong group type. Available only in OpenFlow 1.3.
Bad-Command	Count of error message sent to Controller due to unsupported command. Available only in OpenFlow 1.3.
Bad-Bucket	Count of error message sent to Controller due to error in bucket. Available only in OpenFlow 1.3.
Bad-Watch	Count of error message sent to Controller due to error in watch group. Available only in OpenFlow 1.3.
Permission-Error	Count of error message sent to Controller due permission error. Available only in OpenFlow 1.3.

Table 131. *OpenFlow Statistics*

Parameter	Description
Port-Mod-Failed	
Bad-Port	Count of error messages sent due to invalid port in `port_mod` message.
Bad-hw-addr	Count of error messages sent due to wrong hardware address specified in `port_mod` message.
Bad-Config	Count of error messages sent due to invalid `config` in the `port_mod` message. Available only in OpenFlow 1.3.
Bad-Advertise	Count of error messages sent due to invalid `advertise` in the `port_mod` message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the `port_mod` message. Available only in OpenFlow 1.3.
Switch-Config-Failed	Available only in OpenFlow 1.3
Bad-Flags	Count of error messages sent due to invalid flags in the `switch-config` message. Available only in OpenFlow 1.3.
Permission-Error	Count of error messages sent due to permission error while processing the `switch-config` message. Available only in OpenFlow 1.3.

Management Processor Statistics

The following commands display Management Processor (MP) statistics:

Table 132. *Management Processor Statistics Options*

Command Syntax and Usage
show mp i2c **show processes i2c** Displays Inter-Integrated Circuit (I2C) statistics. **Command mode:** All
show mp memory **show processes memory** Displays memory utilization statistics. **Command mode:** All
show mp packet Displays MP packet statistics.For command options, see page 306. **Command mode:** All
show mp tcp-block **show processes tcp-block** Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 316. **Command mode:** All
show mp thread **show processes thread** Displays thread statistics. **Command mode:** All
show mp udp-block **show processes udp-block** Displays all UDP control blocks that are in use. To view a sample output, see page 317. **Command mode:** All
show processes Displays MP specific statistics. For command options, see page 318. **Command mode:** All
show processes cpu Displays CPU utilization for periods of 1 second, 5 seconds, 1 minute and 5 minutes. To view a sample output and a description of the stats, see page 319. **Command mode:** All

Table 132. *Management Processor Statistics Options*

Command Syntax and Usage
`show processes cpu history` Displays a history of CPU use statistics. To view a sample output, see page 320. **Command mode:** All
`clear mp-counters` Clears all MP statistics. **Command mode:** All

MP Packet Statistics Commands

The following commands display MP Packet statistics:

Table 133. *Packet Statistics Commands*

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leaks and load. To view a sample output and a description of the stats, see page 307. **Command mode:** All
`show mp packet dump {all|rx|tx}` o `all` displays all packet statistics and logs received or sent by the CPU. o `rx` displays all packet statistics and logs received by the CPU. o `tx` displays all packet statistics and logs sent by the CPU. **Command mode:** All
`show mp packet last {both|rx|tx}` *<number of logs (1-1000)>* o `both` displays a list of the most recent packets received or sent by the CPU. o `rx` displays a log of the most recent packets received by the CPU. o `tx` displays a log of the most recent packets sent by the CPU. **Command mode:** All
`show mp packet logs {all|rx|tx}` o `all` displays a log of all packets received or sent by the CPU. o `rx` displays a log of packets received by the CPU. o `tx` displays a log of packets sent by the CPU. **Command mode:** All
`show mp packet parse {rx|tx}` *<parsing option>* Displays a list of received or sent packets that fit the parsing option. For a list of parsing options, see page 312. **Command mode:** All
`show mp packet thread-counters` Displays packet statistics for each thread. To view a sample output, see page 311. **Command mode:** All
`clear mp packet logs` Clears all packet statistics and logs. **Command mode:** Privileged EXEC

MP Packet Statistics

The following command displays MP packet statistics:

`show mp packet counters`

Command mode: All

```
CPU packet statistics at 10:11:10 Wed Oct 22, 2014

 Packet rate:         Incoming            Outgoing
 ------------         --------            --------
 1-second:                 2                   0
 4-seconds:                1                   0
 64-seconds:               2                   0

 Packet counters:     Received               Sent
 ----------------     --------               ----
 Total packets:         359121             289149
 Since bootup:          359121             289149
 BPDUs:                     34             178404
 Cisco packets:              0                  0
 ARP Requests:          100419                  1
 ARP Replies:             4988                  0
 LACP packets:               0                  0
 IPv4 packets:          100394              86826
  ICMP Requests:             0              77321
  ICMP Replies:          77315                  0
  IGMP packets:              0                  0
  PIM packets:               0                  0
  VRRP packets:              0                  0
  TCP  packets:             84                174
   FTP                       0                  0
   HTTP                      0                  0
   SSH                       0                  0
   TACACS                    0                  0
   TELNET                   84                174
   TCP other                 0                  0
  UDP packets:           17666               9331
   DHCP                  13510               5175
   NTP                       3                  3
   PTP                       0                  0
   RADIUS                    0                  0
   SNMP                   4153               4153
   TFTP                      0                  0
   UDP other                 0                  0
  RIP packets:               0                  0
  OSPF packets:              0                  0
  BGP packets:               0                  0
 IPv6 packets:            6647                  8
 LLDP PDUs:               5162              23848
 FCoE FIP PDUs:              0                  0
 ECP PDUs:                   0                 64
 MgmtSock Packets:      192529              86833
 Other:                 141477                 62
```

```
Packet Buffer Statistics:
-------------------------
 allocs:        973757
 frees:         973753
 failures:           0
 dropped:            0

 small packet buffers:
 ---------------------
   current:                1
   max:                 2048
   threshold:            512
   hi-watermark:           2
   hi-water time:   15:11:47 Mon Oct 20, 2014
 medium packet buffers:
 ---------------------
   current:                3
   max:                 2048
   threshold:            512
   hi-watermark:           5
   hi-water time:   15:12:17 Mon Oct 20, 2014

 jumbo packet buffers:
 ---------------------
   current:                0
   max:                   16
   hi-watermark:           0

 pkt_hdr statistics:
 ---------------------
 current          :         0
 max              :      3072
 hi-watermark     :        12
```

The following table describes MP packet statistics.

Table 134. *Packet Statistics*

Statistics	Description
Packets received by CPU	
Total packets	Total number of packets received
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received.
ARP packets	Total number of Address Resolution Protocol packets received.
IPv4 packets	Total number of IPv4 packets received.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
Other	Total number of other packets received.

Table 134. *Packet Statistics (continued)*

Statistics	Description
Packet Buffer Statistics	
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported.
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of medium packet allocations supported.
threshold	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.

Table 134. *Packet Statistics (continued)*

Statistics	Description
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdr statistics	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

Management Processor Packet Thread Statistics

The following command displays Management Processor Packet Thread statistics:

`show mp packet thread-counters`

Command mode: All

```
Per Thread Current Buffer Statistics:
  thid  name      headers       smalls     mediums    jumbos
    1   STEM            0            0           0          0
    2   STP             0            0           0          0
    3   MFDB            0            0           0          0
    4   TND             0            0           0          0
    5   CONS            0            0           0          0
    6   TNET            0            0           0          0
    7   TNET            0            0           0          0
    8   TNET            0            0           0          0
    9   TNET            0            0           0          0
   10   TNET            0            0           0          0
   11   TNET            0            0           0          0
   12   LOG             0            0           0          0
   13   TRAP            0            0           0          0
   14   NTP             0            0           0          0
   15   RMON            0            0           0          0
   18   IP              0            0           0          0
   19   RIP             0            0           0          0
   20   AGR             0            0           0          0
...
   95   OSFM            0            0           0          0
   96   OBSC            0            0           0          0
   97   STPM            0            0           0          0
   98   ARP             0            0           0          0
   99   VMFD            0            0           0          0
  100   NORM            0            0           0          0
  101   DONE            0            0           0          0
      Others            0            0           2          0
```

Logged Packet Statistics

The following command displays logged packets that have been received or sent, based on the specified filter:

show mp packet parse {rx|tx} *<parsing option>*

The filter options are described in the following table.

Table 135. *Packet Log Parsing Options*

Command Syntax and Usage
show mp packet parse {rx|tx} arp Displays only ARP packets logged. **Command mode:** All
show mp packet parse {rx|tx} bgp Displays only BGP packets logged. **Command mode:** All
show mp packet parse {rx|tx} bpdu Displays only BPDUs logged **Command mode:** All
show mp packet parse {rx|tx} cisco Displays only Cisco packets (BPDU/CDP/UDLD) logged. **Command mode:** All
show mp packet parse {rx|tx} dhcp Displays only DHCP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ecp Displays only ECP packets logged. **Command mode:** All
show mp packet parse {rx|tx} fcoe Displays only FCoE FIP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} ftp Displays only FTP packets logged. **Command mode:** All
show mp packet parse {rx|tx} http Displays only HTTP packets logged. **Command mode:** All

Table 135. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} https Displays only HTTPS packets logged. **Command mode:** All
show mp packet parse {rx|tx} icmp Displays only ICMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} igmp Displays only IGMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ip-addr *<IPv4 address>* Displays only logged packets with the specified IPv4 address. **Command mode:** All
show mp packet parse {rx|tx} ipv4 Displays only IPv4 packets logged. **Command mode:** All
show mp packet parse {rx|tx} ipv6 Displays only IPv6 packets logged. **Command mode:** All
show mp packet parse {rx|tx} lacp Displays only LACP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} lldp Displays only LLDP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} mac *<MAC address>* Displays only logged packets with the specified MAC address. **Command mode:** All
show mp packet parse {rx|tx} mgmtsock Displays only packets logged from management ports. **Command mode:** All
show mp packet parse {rx|tx} ntp Displays only NTP packets logged. **Command mode:** All

Table 135. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} ospf Displays only OSPF packets logged. **Command mode:** All
show mp packet parse {rx|tx} other Displays logs of all packets not explicitly selectable. **Command mode:** All
show mp packet parse {rx|tx} pim Displays only PIM packets logged. **Command mode:** All
show mp packet parse {rx|tx} port *<port alias or number>* Displays only logged packets with the specified port. **Command mode:** All
show mp packet parse {rx|tx} radius Displays only RADIUS packets logged. **Command mode:** All
show mp packet parse {rx|tx} rarp Displays only Reverse-ARP packets. **Command mode:** All
show mp packet parse {rx|tx} raw Displays raw packet buffer in addition to headers. **Command mode:** All
show mp packet parse {rx|tx} rip Displays only RIP packets logged. **Command mode:** All
show mp packet parse {rx|tx} snmp Displays only SNMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ssh Displays only SSH packets logged. **Command mode:** All
show mp packet parse {rx|tx} tacacs Displays only TACACS packets logged. **Command mode:** All

Table 135. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} tcp Displays only TCP packets logged. **Command mode:** All
show mp packet parse {rx|tx} tcpother Displays only TCP other-port packets logged. **Command mode:** All
show mp packet parse {rx|tx} telnet Displays only TELNET packets logged. **Command mode:** All
show mp packet parse {rx|tx} tftp Displays only TFTP packets logged. **Command mode:** All
show mp packet parse {rx|tx} udp Displays only UDP packets logged. **Command mode:** All
show mp packet parse {rx|tx} udpother Displays only UDP other-port packets logged. **Command mode:** All
show mp packet parse {rx|tx} vlan *<VLAN ID (1-4095)>* Displays only logged packets with the specified VLAN. **Command mode:** All
show mp packet parse {rx|tx} vrrp Displays only VRRP packets logged. **Command mode:** All

TCP Statistics

The following command displays MP TCP statistics:

`show mp tcp-block`

Command mode: All

```
Data Ports:
--------------------------------------------------------------------------------
All TCP allocated control blocks:
1971dd0c:  0.0.0.0                                        0 <=>
           10.241.31.135                                830 listen MGT up
53ee55f8:  0.0.0.0                                        0 <=>
           0.0.0.0                                      830  listen
53ee5480:  0:0:0:0:0:0:0:0                                0 <=>
           0:0:0:0:0:0:0:0                              830  listen
59c51b00:  0.0.0.0                                        0 <=>
           10.241.31.135                                 80 listen MGT up
144b4670:  0.0.0.0                                        0 <=>
           10.241.31.135                                 23 listen MGT up
144b4aac:  0.0.0.0                                        0 <=>
           127.0.0.1                                     23 listen  up
53ee4c58:  0:0:0:0:0:0:0:0                                0 <=>
           0:0:0:0:0:0:0:0                               23  listen
53ee4ae8:  0.0.0.0                                        0 <=>
           0.0.0.0                                       23  listen

Mgmt Ports:
--------------------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address   State
tcp        0      0 127.0.0.1:5000          *:*               LISTEN
tcp        0      0 10.241.31.135:http      *:*               LISTEN
tcp        0      0 10.241.31.135:telnet    *:*               LISTEN
tcp        0      0 127.0.0.1:680           127.0.0.1:5500    ESTABLISHED
tcp        0      0 127.0.0.1:5000          127.0.0.1:647     ESTABLISHED
tcp        0      0 127.0.0.1:5500          127.0.0.1:680     ESTABLISHED
tcp        0      0 127.0.0.1:647           127.0.0.1:5000    ESTABLISHED
```

The following table describes the MP TCP statistics.

Table 136. *MP Specified TCP Statistics*

Statistics	Description
`14835bd8`	Memory
`0.0.0.0`	Destination IP address
`0`	Destination port
`172.31.38.107`	Source IP
`80`	Source port
`listen`	State

UDP Statistics

The following command displays MP UDP statistics:

`show mp udp-block`

Command mode: All

```
Data Ports:
--------------------------------------------------------------------------
All UDP allocated control blocks:
   68:  listen
  161:  listen

Mgmt Ports:
--------------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address      State
udp        0      0 10.241.31.135:snmp      *:*

0.0.0.0             0 <=> 10.241.31.135     161  accept  MGT  up
```

MP Specific Statistics

The following command displays Management Processor specific statistics:

`show processes`

Command mode: All

```
STEM thread stats:
-------------------------------------------------------------------------------------------
Thread  Thread        Stack         Total     Invoked      Max      Messages  Queue    Status
  ID     Name     Used  /  Max   Runtime(us)   Count   Runtime(us)  in Queue   Hwat
-------------------------------------------------------------------------------------------
   1     STEM                          0        0           0      0                 idle
   2     STP      6968   32768     222279580  1873189        1252      0         3       idle
   3     MFDB     1208    8192      16173562 37397835       29007      0         7       idle
   4     TND      2648    8192       1618648   108104         224      0         3       idle
   5     CONS    12808   61440       1006482   617540       11956      0         1    running
   6     TNET      280   61440             6        1           0      0         1       idle
   7     TNET      280   61440            13        1           0      0         1       idle
   8     TNET      280   61440            13        1           0      0         1       idle
   9     TNET      280   61440            10        1           0      0         1       idle
  10     TNET      280   61440             6        1           0      0         1       idle
  11     TNET      344   61440            18        1           0      0         1       idle
  12     LOG      3016    8192        289492      290        6435      0         3       idle
  13     TRAP     1144    8192         52211   143221          77      0         3       idle
  14     NTP        72    8192             6        1           0      0         1       idle
  15     RMON      232    8192       9450574   932625         350      0         1       idle
  18     IP       6904   32768      55254579   933190         503      0         1       idle
  19     RIP      2520   32768           570      514           0      0         2       idle
  20     AGR      6344  131072        462399    93269          71      0         1       idle
...
  95     OSFM     1208   32768       4882102   932154         338      0         1       idle
  96     OBSC      632    8192       2063098   932634         351      0         1       idle
  97     STPM       72   32768             2        1           0      0         1       idle
  98     ARP      2904   32768     152413220 57155203         347      0         4       idle
  99     VMFD      104   16384             1        1           0      0         1       idle
 100     NORM     1816    4096           958        2           0      0         1       idle
 101     DONE    21384   61440       1115575    11720      166212      0         1       idle
```

CPU Statistics

The following command displays CPU use statistics:

`show processes cpu`

Command mode: All

```
Total CPU Utilization: For 1 second: 0.66%
                       For 5 second: 3.02%
                       For 1 minute: 3.73%
                       For 5 minute: 3.69%
Highest CPU Utilization: thread   5 (CONS) at 14:06:29 Mon Jul  6, 2015
------------------------------------------------------------------------
Thread  Thread                    Utilization                   Status
  ID     Name        1sec       5sec       1Min       5Min
------------------------------------------------------------------------
  1      STEM       0.00%      0.00%      0.00%      0.00%        idle
  2      STP        0.00%      0.00%      0.00%      0.00%        idle
  3      MFDB       0.00%      0.00%      0.00%      0.00%        idle
  4      TND        0.00%      0.00%      0.00%      0.00%        idle
  5      CONS       0.14%      0.04%      0.00%      0.00%     running
  6      TNET       0.00%      0.00%      0.00%      0.00%        idle
...
```

The following table describes the CPU statistics.

Table 137. *CPU Statistics*

Statistics	Description
Thread ID	The thread ID number.
Thread Name	The name of the thread.
1sec	The percent of CPU use over 1 second.
5sec	The percent of CPU use over 5 seconds.
1Min	The percent of CPU use over 1 minute.
5Min	The percent of CPU use over 5 minutes.
Status	The status of the process.

CPU Statistics History

The following command displays a history of CPU use statistics:

`show processes cpu history`

Command mode: All

```
CPU Utilization History
-----------------------------------------
 40 (LACP)   8% at  12:41:07 Mon Jul  6, 2015
 75 (ARP )  32% at  12:41:08 Mon Jul  6, 2015
 75 (ARP )  48% at  12:41:13 Mon Jul  6, 2015
 54 (PROX)  62% at  13:52:06 Mon Jul  6, 2015
 54 (PROX)  63% at  15:03:43 Mon Jul  6, 2015
 54 (PROX)  64% at   4:02:46 Wed Jul  8, 2015
 54 (PROX)  65% at   3:54:27 Thu Jul  9, 2015
```

QoS Statistics

The following commands display QoS statistics:

Table 138. *QoS Statistics Commands*

Command Syntax and Usage
`show qos protocol-packet-control protocol-counters [`<*packet type*>**`]`** Displays the total packet count of the selected packet type received by hardware. The following packet types are allowed: o `802.1x` (IEEE 802.1x packets) o `application-cri-packets` (critical packets of various applications) o `arp-bcast` (ARP broadcast packets) o `arp-ucast` (ARP unicast reply packets) o `bgp` (BGP packets) o `bpdu` (Spanning Tree Protocol packets) o `cisco-bpdu` (Cisco STP packets) o `dest-unknown` (packets with destination not yet learned) o `dhcp` (DHCP packets) o `ecp` (ECP packets) o `fips` (FIPS packets) o `icmp` (ICMP packets) o `icmp6` (ICMP6 packets) o `igmp` (IGMP packets) o `ipv4-miscellaneous` (IPv4 packets with IP options and TTL exception) o `ipv6-nd` (IPv6 Neighbor Discovery packets) o `lacp` (LACP packets) o `lldp` (LLDP packets) o `oflow-cntrler` (packets that hit the OpenFlow send-to-controller filter) o `oflow-default` (packets that hit the OpenFlow default filter) o `oflow-mgmt` (packets that hit the OpenFlow management filter) o `ospf` (OSPF packets) o `ospf3` (OSPF3 Packets) o `pim` (PIM packets) o `ptp` (PTP packets) o `rip` (RIP packets) o `system` (system protocols, such as tftp, ftp, telnet or ssh) o `udld` (UDLD packets) o `vlag` (VLAG packets) o `vrrp` (VRRP packets) **Command mode:** All

Table 138. *QoS Statistics Commands*

Command Syntax and Usage
show qos protocol-packet-control queue-counters **[**<*packet queue number (0-43)*>**|all]** Displays the total number of packets received by each queue. The `all` option displays the number of packets reveived by all queues, including the reserved packet queues. **Command mode:** All
clear qos protocol-packet-control all Clears all packet queue statistics. **Command mode:** Privileged EXEC
clear qos protocol-packet-control protocol-counters **[**<*packet type*>**]** Clears packet queue statistics for the selected packet type. **Command mode:** Privileged EXEC
clear qos protocol-packet-control queue-counters **[**<*packet queue number (0-43)*>**]** Clears packet queue statistics for the selected queue. **Command mode:** Privileged EXEC

Access Control List Statistics

The following commands display ACL statistics:

Table 139. *ACL Statistics Commands*

Command Syntax and Usage
show access-control counters Displays all ACL statistics. **Command mode:** All
show access-control list *<1-256>* **counters** Displays the Access Control List statistics for a specific ACL. **Command mode:** All
show access-control list6 *<1-128>* **counters** Displays the IPv6 ACL statistics for a specific ACL. **Command mode:** All
show access-control macl *<1-256>* **counters** Displays the ACL statistics for a specific management ACL (MACL). **Command mode:** All
show access-control meter *<1-127>* **counters** Displays ACL meter statistics. **Command mode:** All
show access-control vmap *<1-128>* **counters** Displays VLAN Map statistics for the selected VMAP. For a sample display, see page 326. **Command mode:** All
clear access-control list {*<1-256>***|all} counters** Clears ACL statistics. **Command mode:** Privileged EXEC
clear access-control list6 {*<1-128>***|all} counters** Clears IPv6 ACL statistics. **Command mode:** Privileged EXEC
clear access-control macl {*<1-256>***|all} counters** Clears Management ACL (MACL) statistics. **Command mode:** Privileged EXEC

Table 139. *ACL Statistics Commands (continued)*

Command Syntax and Usage
clear access-control meter *<1-127>* **counters** Clears ACL meter statistics. **Command mode:** Privileged EXEC
clear access-control vmap {*<1-128>***} counters** Clears VLAN Map statistics. **Command mode:** Privileged EXEC

ACL Statistics

This option displays ACL statistics.

show access-control counters

Command mode: All

```
Hits for ACL 1:                 26057515
Hits for ACL 2:                 26057497
```

VMAP Statistics

The following command displays VLAN Map statistics.

show access-control vmap *<1-128>* **counters**

Command mode: All

```
Hits for VMAP 1:                    57515
```

Networking Virtualization Statistics

The following table displays Networking Virtualization (NWV) statistics commands.

Table 140. *Networking Virtualization Statistics Commands*

Command Syntax and Usage
show nwv nsx-gw virtual-network [<*VxLAN VNID (1-16777216)*>**] counters** Displays VXLAN Gateway Virtual Network statistics. To view a sample output, see page 328. **Command mode:** All
clear nwv nsx-gw virtual-network [<*VxLAN VNID (1-16777216)*>**] counters** Clears VXLAN Gateway Virtual Network statistics. **Command mode:** Privileged EXEC
show nwv nsx-gw virtual-port [<*port alias or number*>**] counters** Displays VXLAN Gateway virtual port statistics. To view a sample output, see page 328. **Command mode:** All
clear nwv nsx-gw virtual-port [<*port alias or number*>**] counters** Clears VXLAN Gateway virtual port statistics. **Command mode:** Privileged EXEC

VXLAN Gateway Virtual Network Statistics

The following command displays VXLAN Gateway Virtual Network statistics:

show nwv nsx-gw virtual-network counters

Command mode: All

```
VNID        Pkts In       Bytes In   Pkts Out      Bytes Out
-----       -------       --------   --------      ---------
5001        949           99917      1123          5567788
5002        664564        4564446    7235          66799
5003        447           73262      56443         3876234
5004        34564         143693     2345          836252
```

VXLAN Gateway Virtual Port Statistics

The following command displays VXLAN Gateway virtual port statistics:

show nwv nsx-gw virtual-port counters

Command mode: All

```
Port     VNID      Remote TEP       Pkts In    Bytes In    Pkts Out  Bytes Out
-------  --------  --------------   --------   ------------  --------  ---------
 7/1(A)  5174      LOCAL            223        775           6463      56733763
 8/1(A)  5640      LOCAL            114        3894          439       96784
 7/1(A)  5949      LOCAL            663        9044          7333      86673
 6/1(N)  MULTIPLE  192.168.200.15   219555     29550560      219852    29739124
 6/1(N)  MULTIPLE  192.168.200.11   81632033   115262914359  81627786  274699
 6/1(N)  MULTIPLE  192.168.200.12   1269       275486        0         0
```

SNMP Statistics

The following command displays SNMP statistics:

`show snmp-server counters`

Command mode: All

```
SNMP statistics:
snmpInPkts:             150097   snmpInBadVersions:              0
snmpInBadC'tyNames:          0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:          0   snmpEnableAuthTraps:            0
snmpOutPkts:            150097   snmpInBadTypes:                 0
snmpInTooBigs:               0   snmpInNoSuchNames:              0
snmpInBadValues:             0   snmpInReadOnlys:                0
snmpInGenErrs:               0   snmpInTotalReqVars:        798464
snmpInTotalSetVars:       2731   snmpInGetRequests:          17593
snmpInGetNexts:         131389   snmpInSetRequests:            615
snmpInGetResponses:          0   snmpInTraps:                    0
snmpOutTooBigs:              0   snmpOutNoSuchNames:             1
snmpOutBadValues:            0   snmpOutReadOnlys:               0
snmpOutGenErrs:              1   snmpOutGetRequests:             0
snmpOutGetNexts:             0   snmpOutSetRequests:             0
snmpOutGetResponses:    150093   snmpOutTraps:                   4
snmpSilentDrops:             0   snmpProxyDrops:                 0
```

The following tabl describes the SNMP statistics.

Table 141. *SNMP Statistics*

Statistic	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadC'tyNames	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
snmpInBadC'tyUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Table 141. *SNMP Statistics (continued)*

Statistic	Description
snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is *too big.*
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue.`
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.

Table 141. *SNMP Statistics (continued)*

Statistic	Description
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName`.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpOutReadOnlys	Not in use.

Table 141. *SNMP Statistics (continued)*

Statistic	Description
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the OSPFSNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.

NTP Statistics

Enterprise NOS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following command displays NTP statistics:

`show ntp counters`

Command mode: All

```
NTP statistics:
        Primary Server:
                Requests Sent:               17
                Responses Received:          17
                Updates:                     1
        Secondary Server:
                Requests Sent:               0
                Responses Received:          0
                Updates:                     0
        Last update based on response from primary server.
        Last update time:     15:22:05 Wed Nov 28, 2012
        Current system time:   8:05:21 Thu Nov 29, 2012
```

The following table describes the NTP statistics.

Table 142. *NTP Statistics*

Field	Description
Primary Server	• **Requests Sent:** The total number of NTP requests the switch sent to the primary NTP server to synchronize time. • **Responses Received:** The total number of NTP responses received from the primary NTP server. • **Updates:** The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	• **Requests Sent:** The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. • **Responses Received:** The total number of NTP responses received from the secondary NTP server. • **Updates:** The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.

Table 142. *NTP Statistics*

Field	Description
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: **`show ntp counters`**

The following command displays information about NTP associated peers:

`show ntp associations`

Command mode: All

```
 address         ref clock          st    when(s)   offset(s)
*12.200.151.18   198.72.72.10       3     35316     -2
*synced, #unsynced
```

The following table describes the NTP associations statistics.

Table 143. *NTP Associations*

Field	Description
address	Peer address
ref clock	Peer reference clock address
st	Peer stratum
when(s)	Time in seconds since the latest NTP packet was received from the peer
offset(s)	Offset in seconds between the peer clock and local clock

PTP Statistics

The following commands display PTP statistics:

Table 144. *Precision Time Protocol Statistics Commands*

Command Syntax and Usage
show ptp counters Displays Precision Time Protocol statistics. **Command mode:** All
show interface port *<port alias or number>* **ptp-counters** Displays Precision Time Protocol statistics for the port. **Command mode:** All
clear ptp counters Resets PTP packet counters. **Command mode**: Privileged EXEC

Use the following command to display Precision Time Protocol traffic statistics:

show ptp counters

Command mode: All

```
Precision time protocol counters:
+-----------------------------------------+
|Received Announce messages:              0|
|Received Sync messages:                  0|
|Received Follow-Up messages:             0|
|Received Delay-Request messages:         0|
|Received Delay-Response messages:        0|
+-----------------------------------------+
|Sent Announce messages:                  0|
|Sent Sync messages:                      0|
|Sent Follow-Up messages:                 0|
|Sent Delay-Request messages:             0|
|Sent Delay-Response messages:            0|
+-----------------------------------------+
```

PTP statistics include the following:

- Total number of Announce messages transmitted and received.
- Total number of Sync transmitted and received.
- Total number of Follow_Up messages transmitted and received.
- Total number of Delay_Req messages transmitted and received.
- Total number of Delay_Resp messages transmitted and received.

NAT Statistics

The following commands display NAT statistics.

Table 145. *NAT Statistics Commands*

Command Syntax and Usage
show ip nat statistics Displays Network Address Translation (NAT) statistics. **Command mode:** All
clear ip nat statistics Clears NAT statistics. **Command Mode**: Privileged EXEC

Use the following command to display NAT statistics:

show ip nat statistics

Command mode: Privileged EXEC

```
Network address translation status: ENABLED.
Number of hardware source translated packets towards realms:
  inside: 0
  outside: 0
Number of hardware destination translated packets towards realms:
  inside: 0
  outside:0
```

Statistics Dump

The following command dumps switch statistics:

`show counters`

Use the dump command to dump all switch statistics (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the **`dump`** command.

Chapter 4. Configuration Commands

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

Table 146. *General Configuration Commands*

Command Syntax and Usage
copy active-config running-config Copy the active configuration to the current (running) configuration. **Command mode:** Privileged EXEC
copy active-config *<TFTP server filepath>* **[data-port|mgt-port]** Backs up the active configuration to a file on the specified TFTP server. For example: **copy active-config** *tftp://10.72.97.135:/directory/config.txt* **mgt-port** **Command mode:** Privileged EXEC
copy *<TFTP server filepath>* **active-config [data-port|mgt-port]** Restores the active configuration from a file on the specified TFTP server. For example: **copy** *tftp://10.72.97.135:/directory/config.txt* **active-config mgt-port** **Command mode:** Privileged EXEC
copy backup-config running-config Copy the backup configuration to the current (running) configuration. **Command mode:** Privileged EXEC
copy backup-config *<TFTP server filepath>* **[data-port|mgt-port]** Backs up the backup configuration to a file on the specified TFTP server. For example: **copy backup-config** *tftp://10.72.97.135:/directory/config.txt* **mgt-port** **Command mode:** Privileged EXEC
copy *<TFTP server filepath>* **backup-config [data-port|mgt-port]** Restores the backup configuration from a file on the specified TFTP server. For example: **copy** *tftp://10.72.97.135:/directory/config.txt* **backup-config mgt-port** **Command mode:** Privileged EXEC
copy running-config backup-config Copy the current (running) configuration from switch memory to the `backup-config` partition. For details, see page 677. **Command mode:** Privileged EXEC

Table 146. *General Configuration Commands*

Command Syntax and Usage
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the `startup-config` partition. **Command mode:** Privileged EXEC
`copy running-config {ftp|tftp|sftp} [data-port|mgt-port]` Backs up the current (running) configuration to a file on the selected FTP/TFTP/SFTP server. **Command mode:** Privileged EXEC
`copy running-config tftp address` *<TFTP server IP address>* **`filename`** *<TFTP server filepath>* **`[data-port|mgt-port]`** Backs up the current (running) configuration to a file on the specified TFTP server. **Command mode:** Privileged EXEC
`copy running-config` *<TFTP server filepath>* **`[data-port|mgt-port]`** Backs up the current (running) configuration to a file on the specified TFTP server. For example: **`copy running-config`** *tftp://10.72.97.135:/directory/config.txt* **`mgt-port`** **Command mode:** Privileged EXEC
`copy` *<TFTP server filepath>* **`running-config [data-port|mgt-port]`** Restores the current (running) configuration from a file on the specified TFTP server. For example: **`copy`** *tftp://10.72.97.135:/directory/config.txt* **`running-config mgt-port`** **Command mode:** Privileged EXEC
`copy {ftp|tftp|sftp} running-config [data-port|mgt-port]` Restores current configuration from a FTP/TFTP/SFTP server. For details, see page 678. **Command mode:** Privileged EXEC
`copy {tftp|sftp} {ca-cert|host-key|host-cert|public-key}` Import interface used by NIST certified test laboratories for USGv6 (NIST SP 500-267) certification purposes. Required for RSA digital signature authentication verification during IKEv2 interoperability testing. Uses TFTP or SFTP to import: o `ca-cert`: Certificate Authority root certificate o `host-key`: host private key o `host-cert`: host public key o `public-key`: host public key **Command mode:** Privileged EXEC

Table 146. *General Configuration Commands*

Command Syntax and Usage
`copy {ftp|sftp} onie-image [data-port|mgt-port]` Copy an ONIE image from a remote FTP or SFTP server. **Note**: This command is available only after installing the ONIE license key. For more details, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*. **Command mode**: Privileged EXEC
`copy tftp onie-image [address` *<hostname or IP address>*`] [filename`** *<ONIE image fliepath>*`] [data-port|mgt-port]`** Copy an ONIE image from a remote TFTP server. **Note**: This command is available only after installing the ONIE license key. For more details, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*. **Command mode**: Privileged EXEC
`copy onie-image {ftp|sftp} [data-port|mgt-port]` Copy the ONIE image to a remote FTP or SFTP server. **Note**: This command is available only after installing the ONIE license key. For more details, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*. **Command mode**: Privileged EXEC
`copy onie-image tftp [address` *<hostname or IP address>*`] [filename`** *<ONIE image fliepath>*`] [data-port|mgt-port]`** Copy the ONIE image to a remote TFTP server. **Note**: This command is available only after installing the ONIE license key. For more details, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*. **Command mode**: Privileged EXEC
`dir [configs|images]` Displays the configuration files and NOS images currently on the switch. o `configs` - displays only the configuration files currently on the switch o `images` - displays only the system images currently on the switch For more details, see page 34. **Command mode**: Privileged EXEC
`mv` *<source filename> <destination filename>* Copies a configuration files or a system image from the specified location to another specified location. **Note**: This command is applicable only to configuration files or NOS images. **Command mode**: Privileged EXEC

Table 146. *General Configuration Commands*

Command Syntax and Usage
`write [memory]` Copy the current (running) configuration from switch memory to the `active-config` partition. **Command mode:** Privileged EXEC
`show running-config` Dumps current configuration to a script file. For details, see page 676. **Command mode:** Privileged EXEC
`show running-config diff` Displays running configuration changes that have been applied but not saved to flash memory. **Command mode:** Privileged EXEC

Viewing and Saving Changes

As you use the configuration commands to set switch parameters, the changes you make take effect immediately. You do not need to apply them. Configuration changes are lost the next time the switch boots, unless you save the changes.

You can view all running configuration changes that have been applied but not saved to flash memory using the **`show running-config diff`** command in Privileged EXEC mode.

Note: Some operations can override the settings of the Configuration commands. Therefore, settings you view using the Configuration commands (for example, port status) might differ from run-time information that you view using the Information commands. The Information commands display current run-time information of switch parameters.

Saving the Configuration

You must save configuration settings to flash memory, so the G8272 reloads the settings after a reboot.

Note: If you do not save the changes, they will be lost the next time the system is rebooted.

To save the new configuration, enter the following command:

```
RS G8272# copy running-config startup-config
```

or:

```
RS G8272# write
```

Note: The **`write`** command doesn't prompt the user for confirmation.

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reboot, see "Selecting a Configuration Block" on page 710.

System Configuration

These commands provide configuration of switch management parameters such as user and administrator privilege mode passwords, web-based management settings and management access lists.

Table 147. *System Configuration Options*

Command Syntax and Usage
banner *<1-80 characters>* Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the **show sys-info** command. **Command mode:** Global configuration
no banner Deletes the login banner. **Command mode:** Global configuration
[no] boot strict enable Enables or disables switch operation in security strict mode. When enabled, the authentication and privacy protocols and algorithms of the device are compliant with NIST SP-800-131A, with non-complaint protocols and algorithms disabled. **Note:** This setting is applied only after a reboot, during which the device will be reset to default factory configuration. By default, this setting is `disabled`. **Command mode:** Global configuration
easyconnect Allows to apply a series of customizable and predefined configurations based on common deployment scenarios. The EasyConnect (EZC) wizard will display the available configuration options. For more details on using the EZC wizard, see the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*. Command mode: Privileged EXEC
enable password Configures a password required to enter Privileged EXEC command mode. By default, no password is required. **Command mode**: Global configuration
no enable Removes the configured password required to enter Privileged EXEC command mode. **Command mode**: Global configuration

Table 147. *System Configuration Options (continued)*

Command Syntax and Usage
hostname *<1-64 characters>* Enables displaying of the host name (system administrator's name) in the Command Line Interface (CLI). **Command mode:** Global configuration
no hostname Deletes the host name set by the system administrator and displays the default system host name in the CLI. **Command mode:** Global configuration
line console length *<0-300>* Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is 28. **Command mode:** Global configuration
no line console Sets line console length to the default value of 28. **Command mode:** Global configuration
line vty length *<0-300>* Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is 28. **Command mode:** Global configuration
no line vty Sets line vty length to the default value of 28. **Command mode:** Global configuration
[no] prompting Enables or disables CLI confirmation prompts. By default, this settings is enabled. **Note:** When disabled, the switch will choose the default answer. **Command mode:** Global configuration
[no] system bootp Enables or disables the use of the Bootstrap Protocol (BOOTP). If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. For more details, see page 602. The default setting is enabled. **Command mode:** Global configuration

Table 147. *System Configuration Options (continued)*

Command Syntax and Usage
system custom-dst Configures Custom Daylight Saving Time settings. For command options, see page 401. **Command mode:** Global configuration
system date *<yyyy> <mm> <dd>* Prompts the user for the system date. The date retains its value when the switch is rebooted. **Command mode:** Global configuration
[no] system daylight Enables or disables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is `disabled`. **Command mode:** Global configuration
[no] system default-ip {data|mgt} Enables or disables default IP address on data interfaces and management interfaces. The default setting is `enabled`. **Command mode:** Global configuration
[no] system dhcp [hostname|syslog] Enables or disables Dynamic Host Control Protocol for setting the IP address on interface 128. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`. o `hostname` enables or disables hostname option support o `syslog` enables or disables log server option support **Command mode:** Global configuration
system idle *<0-60>* Sets the idle timeout for CLI sessions in minutes. A value of 0 disables the system idle timeout. The default value is `10` minutes. **Command mode:** Global configuration

Table 147. *System Configuration Options (continued)*

Command Syntax and Usage
`system linkscan {fast|normal|slow}` Configures the link scan interval used to poll the status of ports. The values for the different intervals are: o `fast` - 75 miliseconds o `normal` - 150 miliseconds o `slow` - 500 miliseconds **Command mode:** Global configuration
`system notice` *<maximum 2021 character multi-line login notice> <'.' to end>* **`[addline`** *<notice text>***`]`** Displays a login notice immediately before the "Enter password:" prompt. This notice can contain up to 2021 characters and new lines. The `addline` option adds new lines of text to the existing login notice without replacing it. **Command mode:** Global configuration
`no system notice` Deletes the login notice. **Command mode:** Global configuration
`[no] system packet-logging` Enables or disables logging of packets that come to the CPU. The default setting is `enabled`. **Command mode:** Global configuration
`[no] system reset-control` Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. The default setting is `enabled`. **Command mode:** Global configuration
`[no] system server-ports port` *<port alias or number>* Adds or removes the specified port to the list of server ports. For more details, see page 404. **Command mode:** Global configuration
`[no] system service-led enable` Enables (on) or disables (off) the Service Required LED on the front panel of the switch unit. **Command mode:** Global configuration
`[no] system service-led operational-enable` Enables (on) or disables (off) the Service Required LED to glow in steady blue to locate the device. **Command mode:** Privileged EXEC

Table 147. *System Configuration Options (continued)*

Command Syntax and Usage
system time *<hh>:<mm>:<ss>* Configures the system time using a 24-hour clock format. The time retains its value when the switch is rebooted. **Command mode:** Global configuration
system timezone [*<time zone index (1-374)>***]** Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc. The time zone can be directly specified using its unique time zone index. **Command mode:** Global configuration
no system timezone Deletes the time zone configuration. **Command mode:** Global configuration
system usb-eject Allows you to safely remove a USB drive from the USB port, without corrupting files on the drive. **Note:** Not available in stacking. **Command mode:** Global configuration
terminal dont-ask Disables CLI confirmation prompts for the current session. The switch will choose the default answer. By default, CLI confirmation prompts are enabled, if they are not configured differently by using the **prompting** command. **Note:** When using this command any settings configured through the **prompting** command will be temporarily disregarded for the duration of the current session. **Command mode:** All
no terminal dont-ask Enables CLI confirmation prompts for the current session. By default, CLI confirmation prompts are enabled, if they are not configured differently by using the **prompting** command. **Command mode:** All

Table 147. *System Configuration Options (continued)*

Command Syntax and Usage
terminal-length *<0-300>* Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding `line vty length` or `line console length` value in effect at login. **Command mode:** All
ssl minimum-version {tls10|tls11|tls12} Configures the minimum accepted Transport Layer Security (TLS) version. o `tls10` - TLS version 1.0 o `tls11` - TLS version 1.1 o `tls12` - TLS version 1.2 **Command mode:** Global configuration
show boot strict Displays the current security strict mode status. **Command mode:** Global configuration
show system Displays the current system parameters. **Command mode:** All

System License Key Installation

License keys determine the number of available features on the G8272. Each switch comes with a basic license that provides the use of a limited number of functions. On top of the basic license, optional upgrade licenses can be installed to expand the number of available features.

Table 148. *System License Keys Configuration Options*

Command Syntax and Usage
show system | include Serial Displays the Unique ID of the switch that is used to acquire license keys. **Command mode**: All
software-key Enter License Key mode. From this submenu, license keys cam be installed, removed, or copied. **Command mode**: All
enakey address *<hostname or IP address>* **keyfile** *<license key filepath>* **[protocol {tftp|sftp} [data-port|mgt-port]]** Install a license key by copying it from a remote TFTP or SFTP server. **Command mode**: License Key configuration
copy {tftp|sftp} software-key address *<hostname or IP address>* **keyfile** *<license key name>* **[data-port|mgt-port]** Install a license key by copying it from a remote TFTP or SFTP server. **Command mode**: Privileged EXEC
ptkey address *<hostname or IP address>* **key** *<license key name>* **[protocol {tftp|sftp} [file** *<filepath on the server>* **[data-port|mgt-port]]]** Upload an installed license key to a remote TFTP or SFTP server. **Command mode**: License Key configuration
copy software-key address *<hostname or IP address>* **key** *<license key name>* **[protocol {tftp|sftp} [file** *<filepath on the server>* **[data-port|mgt-port]]]** Upload an installed license key to a remote TFTP or SFTP server. **Command mode**: Privileged EXEC
invkeys address *<hostname or IP address>* **[invfile** *<license key filepath>* **[protocol {tftp|sftp} [data-port|mgt-port]]]** Upload inventory installed activation keys to a remote TFTP or SFTP server. **Command mode**: License Key configuration
copy invkeys address *<hostname or IP address>* **[invfile** *<license key filepath>* **[protocol {tftp|sftp} [data-port|mgt-port]]]** Upload inventory installed activation keys to a remote TFTP or SFTP server. **Command mode**: Privileged EXEC

Table 148. *System License Keys Configuration Options*

Command Syntax and Usage
rmkey key *<license key name>* Removes an installed license key from the switch. **Command mode**: License Key configuration
show software-key Displays the license keys currently installed on the switch. **Command mode**: All

System Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 149. *Error Disable Configuration Options*

Command Syntax and Usage
`[no] errdisable recovery` Globally enables or disables automatic error-recovery for error-disabled ports. The default setting is `disabled`. **Note**: Each port must have error-recovery enabled to participate in automatic error recovery. **Command mode:** Global configuration
`errdisable timeout` *<30-86400>* Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is `300` seconds. **Note**: When you change the timeout value, all current error-recovery timers are reset. **Command mode:** Global configuration
`show errdisable` Displays the current system Error Disable configuration. For more command options, see page 37. **Command mode:** All

Link Flap Dampening Configuration

The Link Flap Dampening feature allows the switch to automatically disable a port if too many link flaps (link up/link down) are detected on the port during a specified time interval. The port remains in the error-disabled state until it is re-enabled manually or re-enabled automatically by the switch after a timeout period has elapsed.

Table 150. *Link Flap Dampening Configuration Options*

Command Syntax and Usage
`[no] errdisable link-flap enable` Enables or disables Link Flap Dampening. **Command mode**: Global configuration
`errdisable link-flap max-flaps` *<1-100>* Configures the maximum number of link flaps allowed in the configured time period. The default value is `5`. **Command mode**: Global configuration
`errdisable link-flap time` *<5-500>* Configures the time period, in seconds. The default value is `30` seconds. **Command mode**: Global configuration
`show errdisable link-flap` Displays the current Link Flap Dampening parameters. **Command mode**: All

System Host Log Configuration

The following table describes the System Host Log commands.

Table 151. *Host Log Configuration Options*

Command Syntax and Usage
logging buffer severity *<0-7>* Sets the severity level of the syslog messages saved to flash memory. The default is 7, which means log all severity levels. **Command mode:** Global configuration
no logging buffer severity Disables the saving of syslog messages to the flash memory. **Command mode:** Global configuration
[no] logging console Enables or disables delivering syslog messages to the console. The default setting is `enabled`. **Note:** When necessary, disabling `console` logging ensures the switch is not affected by syslog messages. **Command mode:** Global configuration
logging console severity *<0-7>* This option sets the severity level of syslog messages delivered via the console, telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed. The default is 7, which means log all severity levels. **Command mode:** Global configuration
no logging console severity Disables delivering syslog messages to the console based on severity. **Command mode:** Global configuration
logging host *<1-2>* **address** *<IPv4 address>* Sets the IP address of the first or second syslog host. **Command mode:** Global configuration
logging host *<1-2>* **address6** *<IPv6 address>* Sets the IPv6 address of the first or second syslog host. **Command mode:** Global configuration
logging host *<1-2>* **{data-port|mgt-port}** Sets the port of the first or second syslog host. **Command mode:** Global configuration

Table 151. *Host Log Configuration Options (continued)*

Command Syntax and Usage
logging host *<1-2>* **facility** *<0-7>* This option sets the facility level of the first or second syslog host displayed. The default value is `0`. **Command mode:** Global configuration
logging host *<1-2>* **port** *<UDP port (1-65535)>* Configure the UDP server port used by the syslog host to receive logging messages from the switch. **Command mode**: Global configuration
logging host *<1-2>* **severity** *<0-7>* This option sets the severity level of the first or second syslog host displayed. The default value is `7`, which means log all severity levels. **Command mode:** Global configuration
no logging host *<1-2>* Deletes the specified syslog host. **Command mode:** Global configuration
[no] logging log {all|*<feature>***}** Enables or disables features for which syslog messages can be generated. You can choose to enable/disable syslog on all available features by using the option `all` or enable/disable specific features (such as `vlans`, `stg` or `ssh`). For a complete list of features, see page 357. **Command mode:** Global configuration
[no] logging pdrop enable Enables or disables packet drop logging. By default, the switch generates these messages once every `2` minutes. **Command mode:** Global configuration
logging pdrop interval *<0-30>* Configures the packet drop logging interval, in minutes. The default value is `2` minutes. **Command mode:** Global configuration
logging source-interface loopback *<1-5>* Sets the loopback interface number for syslogs. **Command mode:** Global configuration
no logging source-interface loopback Removes the loopback interface for syslogs. **Command mode:** Global configuration

Table 151. *Host Log Configuration Options (continued)*

Command Syntax and Usage
`[no] logging synchronous [level {`*<0-7>***`|all}]`** Enables or disables synchronous logging messages. When enabled, logging messages are displayed synchronously. The `level` parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. The `all` option displays all messages asynchronously, regardless the severity level. The default setting is `2`. **Command mode:** Global configuration
`show logging [messages] [severity` *<0-7>***`] [reverse] [|{include|exclude|section|begin|head`** *<1-2000>***`|`** **`|last`** *<1-2000>***`}]`** Displays the current syslog settings, followed by the most recent 2000 syslog messages. o `messages` displays the most recent 2000 syslog messages only o `severity` displays syslog messages of the specified severity level o `reverse` displays syslog messages starting with the most recent message o `|` displays syslog messages that match one of the following filters: • `include` displays syslog messages that match the specified expression • `exclude` displays syslog messages that don't match the specified expression • `section` displays syslog messages that match the specified section • `begin` displays syslog messages beginning from the first message that matches the specified expression • `head` displays the oldest syslog messages for the specified value • `last` displays the most recent syslog messages for the specified value For details, see page 48. **Command mode:** All

The following list displays the features available for the **`[no] logging log`** command:

- `arp-inspection` - Dynamic ARP Inspection logging
- `bgp` - BGP logging
- `cfg` - Configuration logging
- `cfgchg` - Configuration Change logging
- `cli` - Command Line Interface logging
- `console` - Console logging
- `dcbx` - DCB Capability Exchange logging
- `difftrak` - Configuration Difference Tracking logging
- `dot1x` - 802.1x logging
- `failover` - Failover logging
- `fcf` - FCF logging
- `fcoe` - Fibre Channel over Ethernet logging
- `hotlinks` - Hot Links logging
- `igmp-group` - IGMP group logging
- `igmp-mrouter` - IGMP mrouter logging
- `igmp-querier` - IGMP querier logging
- `ip` - Internet Protocol version 4 logging
- `ipv6` - Internet Protocol version 6 logging
- `lacp` - Link Aggregation Control Protocol logging
- `link` - System Port Link logging
- `lldp` - LLDP logging
- `management` - Management logging
- `mld` - MLD logging
- `nat` - Network Address Translation logging
- `netconf` - NETCONF Configuration Protocol logging
- `ntp` - Network Time Protocol logging
- `openflow` - Openflow logging
- `ospf` - OSPF logging
- `ospfv3` - OSPF version 3 logging
- `private-vlan` - Private VLAN logging
- `ptp` - Precision Time Protocol logging
- `rmon` - Remote Monitoring logging
- `scheduler` - Scheduler module logging
- `script` - Script module logging

- `server` - Syslog server logging
- `slp` - Service Location Protocol logging
- `spanning-tree-group` - Spanning tree group logging
- `ssh` - Secure Shell logging
- `system` - System logging
- `ufp` - UFP logging
- `vlag` - Virtual Link Aggregation logging
- `vlan` - VLAN logging
- `vm` - Virtual Machine logging
- `vrrp` - Virtual Router Redundancy Protocol logging
- `web` - Web logging

SSH Server Configuration

For the RackSwitch G8272, these commands enable Secure Shell access from any SSH client.

Table 152. *SSH Server Configuration Options*

Command Syntax and Usage
`[no] ssh enable` Enables or disables the SSH server. **Command mode:** Global configuration
`ssh generate-host-key` Generate the RSA host key. **Command mode:** Global configuration
`ssh maxauthattempts` *<1-20>* Sets the maximum number of SSH authentication attempts. The default value is `2`. **Command mode:** Global configuration
`no ssh maxauthattempts` Resets the maximum number of SSH authentication attempts to its default value of `2`. **Command mode:** Global configuration
`ssh port` *<TCP port number (1-65535)>* Sets the SSH server port number. The default port number is `22`. **Command mode:** Global configuration
`no ssh port` Resets the SSH server port to the default port number - `22`. **Command mode:** Global configuration
`ssh public-key index` *<1-100>* **`{adduser|deluser} username`** *<user name>* Assigns another user name for existing public keys or removes a user name. **Command mode:** Global configuration
`[no] ssh scp-enable` Enables or disables the SCP apply and save. **Command mode:** Global configuration
`ssh scp-password` Set the administration password for SCP access. **Command mode:** Global configuration

Table 152. *SSH Server Configuration Options (continued)*

Command Syntax and Usage
show ssh Displays the current SSH server configuration. **Command mode:** All
show ssh-clienthostkey {address *<SFTP server IP address>***|all}** Displays the current SFTP/SSH host key configuration. o `address:` Displays a specific SFTP/SSH host key o `all:` Displays all SFTP/SSH host keys **Commands mode:** All
show ssh-clientpubkey {all|index *<1-100>***|username** *<user name>***}** Displays the current SSH public key configuration. o `all:` Displays all SSH public keys o `index:` Displays a specific SSH public key o `username:` Displays all the SSH public keys of a particular user **Command mode:** All
clear ssh-clienthostkey {address *<SFTP server IP address>***|all}** Clears stored SFTP/SSH host key configuration. o `address:` Clears a specific SFTP/SSH host key o `all:` Clears all SFTP/SSH host keys **Command mode:** Privileged EXEC
clear ssh-clientpubkey {all|index *<1-100>***|username** *<user name>***}** Clears stored public key configuration. o `all:` Clears all SSH public keys o `index:` Clears a specific SSH public key o `username:` Clears a particular username from all the SSH public keys **Command mode:** Privileged EXEC

RADIUS Server Configuration

The following table describes the RADIUS Server commands.

Table 153. *RADIUS Server Configuration Options*

Command Syntax and Usage
[no] radius-server backdoor Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password for your switch, contact your Service and Support line. **Command mode:** Global configuration
[no] radius-server enable Enables or disables the RADIUS server. **Command mode:** Global configuration
radius-server port *<UDP port number (1500-3000)>* Configures the RADIUS server port. Enter the number of the UDP port to be configured. The default port is `1645`. **Command mode:** Global configuration
default radius-server port Resets the RADIUS server port to the default UDP port - `1645`. **Command mode:** Global configuration
radius-server primary-host {*<hostname>***|***<IP address>***} key** *<1-32 characters>* Sets the primary RADIUS server address and the shared secret between the switch and the RADIUS server(s). **Command mode:** Global configuration
radius-server primary-host {data-port|mgt-port} Defines the primary interface port to use to send RADIUS server requests. Select the port to use for data transfer. **Command mode:** Global configuration
no radius-server primary-host [key] Deletes the primary RADIUS server. The `key` option only deletes the shared secret between the switch and the RADIUS server. **Command mode:** Global configuration
radius-server retransmit *<1-3>* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is `3` requests. **Command mode:** Global configuration

Table 153. *RADIUS Server Configuration Options (continued)*

Command Syntax and Usage
radius-server secondary-host {<*hostname*>**|**<*IP address*>**} key** <*1-32 characters*> Sets the secondary RADIUS server address and the shared secret between the switch and the RADIUS server(s). **Command mode:** Global configuration
radius-server secondary-host {data-port|mgt-port} Defines the secondary interface port to use to send RADIUS server requests. Select the port to use for data transfer. **Command mode:** Global configuration
[no] radius-server secondary-host [key] Deletes the secondary RADIUS server. The `key` option only deletes the shared secret between the switch and the RADIUS server. **Command mode:** Global configuration
[no] radius-server secure-backdoor Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor is enabled. **Command mode:** Global configuration
radius-server timeout *<1-10>* Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is `3` seconds. **Command mode:** Global configuration
ip radius source-interface loopback *<1-5>* Sets the RADIUS source loopback interface. **Command mode:** Global configuration
no ip radius source-interface loopback Removes all RADIUS source loopback interfaces. **Command mode:** Global configuration
show radius-server Displays the current RADIUS server parameters. **Command mode:** All

TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. Both TACACS and TACACS+ are described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization and accounting.

Table 154. *TACACS+ Server Configuration Options*

Command Syntax and Usage
`[no] tacacs-server accounting-enable` Enables or disables TACACS+ accounting. **Command mode:** Global configuration
`tacacs-server attempts` *<1-10>* Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts. **Command mode:** Global configuration
`no tacacs-server attempts` Resets the number of failed login attempts to the default value of 2. **Command mode:** Global configuration
`[no] tacacs-server backdoor` Enables or disables the TACACS+ back door for Telnet, SSH/SCP or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default setting is `disabled`. To obtain the TACACS+ backdoor password for your G8272, contact your Service and Support line. **Command mode:** Global configuration

Table 154. *TACACS+ Server Configuration Options (continued)*

Command Syntax and Usage
tacacs-server chpassp *<1-32 characters>* Defines the password for the primary TACACS+ server. **Command mode:** Global configuration
tacacs-server chpasss *<1-32 characters>* Defines the password for the secondary TACACS+ server. **Command mode:** Global configuration
[no] tacacs-server command-authorization Enables or disables TACACS+ command authorization. **Command mode:** Global configuration
[no] tacacs-server command-logging Enables or disables TACACS+ command logging. **Command mode:** Global configuration
tacacs-server directed-request [no-truncate|restricted] Enables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, `username@hostname`) during login. This command allows the following options: o `restricted`: Only the username is sent to the specified TACACS+ server. o `no-truncate`: The entire login string is sent to the TACACS+ server. **Command mode:** Global configuration
no tacacs-server directed-request Disables TACACS+ directed request. **Command mode:** Global configuration
[no] tacacs-server enable Enables or disables the TACACS+ server. By default, the server is `disabled`. **Command mode:** Global configuration
[no] tacacs-server enable-bypass Enables or disables the enable-bypass for administrator privilege. By default, enable-bypass is `enabled`. **Command mode:** Global configuration
[no] tacacs-server encryption-enable Enables or disables the encryption of TACACS+ packets. **Command mode:** Global configuration

Table 154. *TACACS+ Server Configuration Options (continued)*

Command Syntax and Usage
[no] tacacs-server password-change Enables or disables TACACS+ password change. The default value is `disabled`. **Command mode:** Global configuration
tacacs-server port *<TCP port number (1-65000)>* Enter the number of the TCP port to be configured. The default is `49`. **Command mode:** Global configuration
default tacacs-server port Resets the TACACS+ server port to the default port number - `49`. **Command mode:** Global configuration
tacacs-server primary-host {*<hostname>***|***<IP address>***} key** *<1-32 characters>* Sets the primary TACACS+ server address and the shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
tacacs-server primary-host {data-port|mgt-port} Defines the primary interface port to use to send TACACS+ server requests. Select the port to use for data transfer. **Command mode:** Global configuration
no tacacs-server primary-host [key] Deletes the primary TACACS+ server. The `key` option only removes the shared secret between the switch and the TACACS+ server. **Command mode:** Global configuration
[no] tacacs-server privilege-mapping Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`. **Command mode:** Global configuration
tacacs-server retransmit *<1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is `3` requests. **Command mode:** Global configuration

Table 154. *TACACS+ Server Configuration Options (continued)*

Command Syntax and Usage
tacacs-server secondary-host {<*hostname*>**|**<*IP address*>**} key** <*1-32 characters*> Sets the secondary TACACS+ server address and the shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
tacacs-server secondary-host [data-port|mgt-port] Defines the secondary interface port to use to send TACACS+ server requests. Select the port to use for data transfer. **Command mode:** Global configuration
no tacacs-server secondary-host [key] Deletes the secondary TACACS+ server. The `key` option only removes the shared secret between the switch and the TACACS+ server. **Command mode:** Global configuration
[no] tacacs-server secure-backdoor Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default is `disabled`. **Command mode:** Global configuration
tacacs-server timeout <*4-15*> Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is `5` seconds. **Command mode:** Global configuration
tacacs-server user-mapping <*0-15*> **{user|oper|admin}** Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level. **Command mode:** Global configuration
no tacacs-server user-mapping <*0-15*> Removes a TACACS+ authorization level. **Command mode:** Global configuration
ip tacacs source-interface loopback <*1-5*> Sets the TACACS+ source loopback interface. **Command mode:** Global configuration

Table 154. *TACACS+ Server Configuration Options (continued)*

Command Syntax and Usage
no ip tacacs source-interface loopback Deletes all TACACS+ source loopback interfaces. **Command mode:** Global configuration
primary-password Configures the password for the primary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
secondary-password Configures the password for the secondary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
show tacacs-server Displays current TACACS+ configuration parameters. **Command mode:** All

LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

Table 155. *LDAP Server Configuration Options*

Command Syntax and Usage
`ldap-server mode {enhanced|legacy}` Configures the LDAP client mode. o `legacy` - provides LDAP version 1 (LDAPv1) client functionality o `enhanced` - provides LDAP versions 2 and 3 (LDAPv2, LDAPv3) client functionality The default mode is `legacy`. **Note**: When switching between LDAP client modes, LDAP configurations made before the change are lost. **Command mode**: Global configuration
`ldap-server attribute group` *<1-128 characters>* Configures a customized LDAP group search attribute, where the group membership information of the user is stored. The default value is `memberOf`. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server attribute group` Resets the LDAP group search attribute to its default value of `memberOf`. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server attribute login-permission` *<1-128 characters>* Configures a customized LDAP login permission attribute, where the user's or the group's permission string is stored. The default value is `ibm-chassisRole`. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server attribute login-permission` Resets the LDAP login permission attribute to its default value of `ibm-chassisRole`. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`ldap-server attribute username` *<1-128 characters>* Configures a customized LDAP user search attribute. The default value is `uid` (unique identification number). **Note**: The user attribute needs to be set to `cn` (common name) if LDAP server is MS active directory. For example: `cn=John Smith` **Command mode:** Global configuration
`no ldap-server attribute username` Resets the LDAP user search attribute to its default value of `uid`. **Command mode:** Global configuration
`no ldap-server attribute` Resets the LDAP attributes to their default values. **Command mode**: Global configuration
`[no] ldap-server backdoor` Enables or disables the LDAP back door for Telnet, SSH, SCP, HTTP, or HTTPS access. The default setting is `disabled`. **Note**: To obtain the LDAP back door password for your G8272, contact your Service and Support line. **Command mode:** Global configuration
`ldap-server basedn` *<1-128 characters>* Configure the Distinguished Name (DN) of the LDAP server. The DN consists of a sequence of different Relative Distinguished Names (RDN) connected by commas. An RDN is an attribute that has an associated value in the format '`attribute`=*value*'. For a list of typical RDNs, see page 374. Enter the full path for your organization. For example: `ou=people,dc=mydomain,dc=com` **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server basedn` Deletes the configured DN. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`ldap-server bind-mode {login|pre-config|sasl}` Configures the bind request method used by the LDAP client for authentication. It also configures the LDAP version used. The LDAP server will allow only authenticated LDAP clients to search or retrieve directory entries stored on the server. o `login` - configures the switch to use login credentials when sending a bind request. The LDAP client will construct a DN using the username and other fields, such as the domain name or the user search attribute. o `pre-config` - configures the switch to use credentials specified via the **`ldap-server binddn`** command when sending a bind request. o `sasl` - configures the switch to use Simple Authentication and Secure Layer (SASL) when sending a bind request. The default bind request method is `login`. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server binddn {dn` *<1-64 characters>***`|key`** *<1-32 characters>***`}`** Configures a customized distinguished name (DN) and password. This creates a set of pre-configured credentials that can be used for authentication when sending a bind request to the LDAP server. **Note**: The credentials configured through this command are used only when the switch bind mode is set to `pre-config`. If the bind mode is set to `login`, any credentials configured through this command are ignored. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server binddn` Deletes the pre-configured credentials. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server domain` *<1-128 characters>* Sets the domain name for the LDAP server. Enter the full path for your organization. For example: `ou=people,dc=mydomain,dc=com` **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`no ldap-server domain` Removes the LDAP server domain name. **Command mode:** Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`[no] ldap-server enable` Enables or disables the LDAP server. **Command mode:** Global configuration
`ldap-server group-filter` *<LDAP groups>* Configures a list of LDAP groups to be searched for login permissions. Multiple groups must be separated by commas. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server group-filter` Removes the list of LDAP groups searched for login permissions. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server host` *<LDAP server number (1-4)> <IP address or hostname>* **`[port`** *<UDP port number(1-65535)>***`] [data-port|mgt-port]`** Configures up to four external LDAP servers. The default UDP port used by LDAP is `389`. **Note**: The IP address and port number of a LDAP server must be non-zero. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`no ldap-server host` *<LDAP server number (1-4)>* Removes the specified external LDAP server. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server port` *<UDP port number (1-65000)>* Enter the number of the UDP port to be configured. The default port is `389`. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`default ldap-server port` Resets the LDAP server port to the default port number - `389`. **Command mode:** Global configuration
`ldap-server primary-host` *<IPv4 address>* **`[data-port|mgt-port]`** Configures the primary LDAP server with an IPv4 address. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`no ldap-server primary-host` Deletes the primary LDAP server. **Command mode:** Global configuration
`ldap-server ipv6 primary-host` *<IPv6 address>* **`[data-port| |mgt-port]`** Configures the primary LDAP server with an IPv6 address. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`no ldap-server ipv6 primary-host` Deletes the primary LDAP server. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`ldap-server retransmit` *<1-3>* Sets the number of failed authentication requests before switching to a different LDAP server. The default is `3` requests. **Command mode:** Global configuration
`ldap-server security clear` Configures LDAP to not encrypt LDAP credentials (DN and password) when sending a bind request to the LDAP server. The default security mode is `clear` (clear text). **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server security ldaps` Configures LDAP to encrypt LDAP credentials (DN and password) using Secure LDAP (LDAPS) when sending a bind request to the LDAP server. This requires the LDAP client to present a Certificate Authority (CA) root certificate. The CA root certificate can be downloaded from the LDAP server. For more details, see page 340. The LDAP client and LDAP server must initiate a separate Transport Layer Security (TLS) session before any LDAP messages are exchanged. This is usually achieved on UDP port 636. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`ldap-server security starttls` Configures LDAP to encrypt LDAP credentials (DN and password) using Start Transport Layer Security (StartTLS) when sending a bind request to the LDAP server. This requires the LDAP client to present a Certificate Authority (CA) root certificate. The CA root certificate can be downloaded from the LDAP server. For more details, see page 340. The LDAP client and LDAP server do not need to initiate a separate TLS session before any LDAP messages are exchanged. StartTLS encrypts a non-encrypted LDAP connection by wrapping it with TLS at any time during or after the connection has been established. Thus, there is no need to use a separate port for encrypted LDAP communication. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`[no] ldap-server security mutual` Enables or disables LDAP to request the LDAP server to also provide its own Certificate Authority (CA) root certificate for authentication by the LDAP client. The LDAP server and the LDAP client both compare the other's CA root certificate against their own. If both certificates match, the authentication succeeds. If either certificate does not match, the authentication fails. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`[no] ldap-server srv` Enables or disables the switch to look up LDAP server information by retrieving a Service (SRV) record associated with LDAP from the configured Domain Name System (DNS). For more details on DNS, see "Domain Name System Configuration" on page 600. **Note**: This option is available only in LDAP enhanced mode. **Command mode**: Global configuration
`ldap-server secondary-host` *<IPv4 address>* **`[data-port|mgt-port]`** Configures the secondary LDAP server with an IPv4 address. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`no ldap-server secondary-host` Deletes the secondary LDAP server. **Command mode:** Global configuration
`ldap-server ipv6 secondary-host` *<IPv6 address>* **`[data-port| |mgt-port]`** Configures the secondary LDAP server with an IPv6 address. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration

Table 155. *LDAP Server Configuration Options (continued)*

Command Syntax and Usage
`no ldap-server ipv6 secondary-host` Deletes the secondary LDAP server. **Note**: This option is available only in LDAP legacy mode. **Command mode:** Global configuration
`ldap-server timeout` *<4-15>* Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is `5` seconds. **Command mode:** Global configuration
`show ldap-server` Displays the current LDAP server parameters. For more details, see page 50. **Command mode:** All except User EXEC

Typical RDNs include the following:

- `dc` (domain component). For example: dc=lenovo,dc=com
- `cn` (common name). For example: cn=John Smith
- `ou` (organization unit name). For example: ou=development
- `o` (organization name). For example: o=Lenovo
- `street` (street name). For example: street=Baker
- `l` (locality name). For example: l=London
- `st` (state or province name). For example: st=London
- `c` (country name). For example: c=England
- `uid` (user ID). For example: uid=329800735698586629295641978511506172918

NTP Server Configuration

These commands allow you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is `disabled`.

Table 156. *NTP Server Configuration Options*

Command Syntax and Usage
`[no] ntp enable` Enables or disables the NTP synchronization service. **Command mode:** Global configuration
`ntp interval` *<5-44640>* Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server. The default value is `1440`. **Command mode:** Global configuration
`ntp ipv6 primary-server {data-port|mgt-port}` Prompts for the port of the IPv6 primary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`ntp ipv6 primary-server` *<IPv6 address>* **`[data-port|mgt-port]`** Prompts for the IPv6 address of the primary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`no ntp ipv6 primary-server` Deletes the IPv6 primary NTP server. **Command mode:** Global configuration
`ntp ipv6 secondary-server {data-port|mgt-port}` Prompts for the port of the IPv6 secondary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`ntp ipv6 secondary-server` *<IPv6 address>* **`[data-port|mgt-port]`** Prompts for the IPv6 address of the secondary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
`no ntp ipv6 secondary-server` Deletes the IPv6 secondary NTP server. **Command mode:** Global configuration

Table 156. *NTP Server Configuration Options (continued)*

Command Syntax and Usage
ntp primary-server {data-port|mgt-port} Prompts for the port of the primary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
ntp primary-server *<hostname or IP address>* **[data-port|mgt-port]** Prompts for the IP address or host name of the primary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
no ntp primary-server Deletes the primary NTP server. **Command mode:** Global configuration
ntp offset *<0-86400>* Configures the minimum offset in seconds between the switch clock and the NTP server that triggers a system log message. The default value is **300** seconds. **Command mode:** Global configuration
no ntp offset Resets the NTP offset to the default **300** seconds value. **Command mode:** Global configuration
ntp secondary-server {data-port|mgt-port} Prompts for the port of the secondary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
ntp secondary-server *<hostname or IP address>* **[data-port|mgt-port]** Prompts for the IP address or host name of the secondary NTP server to which you want to synchronize the switch clock. **Command mode:** Global configuration
no ntp secondary-server Deletes the secondary NTP server. **Command mode:** Global configuration
ntp source loopback *<1-5>* Sets the NTP source loopback interface. **Command mode:** Global configuration
no ntp source loopback Deletes all NTP source loopback interface. **Command mode:** Global configuration

Table 156. *NTP Server Configuration Options (continued)*

Command Syntax and Usage
[no] ntp sync-logs Enables or disables informational logs for NTP synchronization failures. Default setting is `enabled`. **Command mode:** Global configuration
show ntp Displays the current NTP service settings. **Command mode:** All

System SNMP Configuration

Enterprise NOS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 157. *System SNMP Options*

Command Syntax and Usage
`[no] snmp-server authentication-trap enable` Enables or disables the use of the system authentication trap facility. The default setting is `disabled`. **Command mode:** Global configuration
`snmp-server contact` *<1-64 characters>* Configures the name of the system contact. The contact can have a maximum of 64 characters. **Command mode:** Global configuration
`no snmp-server contact` Deletes the name of the system contact. **Command mode:** Global configuration
`snmp-server host` *<trap host IP address> <trap host community string (1-33 characters)>* Adds a trap host server. **Command mode:** Global configuration

Table 157. *System SNMP Options (continued)*

Command Syntax and Usage
no snmp-server host *<trap host IP address>* Removes the trap host server. **Command mode:** Global configuration
[no] snmp-server link-trap [port] *<port alias or number>* **enable** Enables or disables the sending of SNMP link up and link down traps for a specific system port. The default setting is `disabled`. **Command mode:** Global configuration
snmp-server location *<1-64 characters>* Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode:** Global configuration
no snmp-server location Deletes the name of the system location. **Command mode:** Global configuration
snmp-server name *<1-64 characters>* Configures the name for the system. The name can have a maximum of 64 characters. **Command mode:** Global configuration
no snmp-server name Deletes the name of the system. **Command mode:** Global configuration
snmp-server read-community *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is *public*. **Command mode:** Global configuration
[no] snmp-server read-community-additional *<1-32 characters>* Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported. **Command mode:** Global configuration
snmp-server timeout *<1-30>* Sets the timeout value for the SNMP state machine, in minutes. **Command mode:** Global configuration

Table 157. *System SNMP Options (continued)*

Command Syntax and Usage
snmp-server trap-source {<*IP interface number*>**|loopback** <*1-5*>**}** Configures the source interface for SNMP traps. To send traps through the management ports, specify interface 126. **Command mode:** Global configuration
no snmp-server trap-source [loopback] Deletes all source interfaces for SNMP traps. The `loopback` option only removes the loopback source interfaces. **Command mode:** Global configuration
snmp-server write-community <*1-32 characters*> Configures the SNMP write community string. The write community string controls SNMP "set" access to the switch. It can have a maximum of 32 characters. The default write community string is *private*. **Command mode:** Global configuration
[no] snmp-server write-community-additional <*1-32 characters*> Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported. **Command mode:** Global configuration
show snmp-server Displays the current SNMP configuration. **Command mode:** All

SNMPv3 Configuration

SNMP version 3 (SNMPv3) is an extensible SNMP Framework that supplements the SNMPv2 Framework by supporting the following:

- a new SNMP message format
- security for messages
- access control
- remote configuration of SNMP parameters

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

Table 158. *SNMPv3 Configuration Options*

Command Syntax and Usage
snmp-server access *<1-32>* This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view command options, see page 385. **Command mode:** Global configuration
snmp-server community *<1-16>* The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view command options, see page 387. **Command mode:** Global configuration
snmp-server group *<1-17>* A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view command options, see page 386. **Command mode:** Global configuration
snmp-server notify *<1-16>* A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view command options, see page 390. **Command mode:** Global configuration
snmp-server target-address *<1-16>* This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view command options, see page 388. **Command mode:** Global configuration

Table 158. *SNMPv3 Configuration Options (continued)*

`snmp-server target-parameters` *<1-16>* This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view command options, see page 389. **Command mode:** Global configuration
`snmp-server user` *<1-17>* This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view command options, see page 383. **Command mode:** Global configuration
`snmp-server view` *<1-128>* This command allows you to create different MIB views. To view command options, see page 384. **Command mode:** Global configuration
`show snmp-server v3` Displays the current SNMPv3 configuration. **Command mode:** All

User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Table 159. *User Security Model Configuration Options*

Command Syntax and Usage
snmp-server user *<1-17>* **authentication-protocol {md5|sha|none} authentication-password** This command allows you to configure the authentication protocol and password. The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96 for compatibility mode, HMAC-SHA-96 for security strict mode or none. The default algorithm is `none`. `MD5` authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility. When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication. **Command mode:** Global configuration
snmp-server user *<1-17>* **name** *<1-32 characters>* This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch. **Command mode:** Global configuration
snmp-server user *<1-17>* **privacy-protocol {des|aes|none} privacy-password** This command allows you to configure the type of privacy protocol and the privacy password. The privacy protocol protects messages from disclosure. The options are: o `des` (CBC-DES Symmetric Encryption Protocol) o `aes` (AES-128 Advanced Encryption Standard Protocol) o `none` If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). In security strict mode, if you do not select SNMPv3 account backward compatibility, only `des` privacy protocol is supported. If you specify `aes` as the privacy protocol, make sure that you have selected HMAC-SHA-96 authentication protocol. If you select `none` as the authentication protocol, you will get an error message. You can create or change the privacy password. **Command mode:** Global configuration

Table 159. *User Security Model Configuration Options*

Command Syntax and Usage
no snmp-server user *<1-17>* Deletes the USM user entries. **Command mode:** Global configuration
show snmp-server v3 user *<1-17>* Displays the USM user entries. **Command mode:** All

SNMPv3 View Configuration

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

Table 160. *SNMPv3 View Configuration Options*

Command Syntax and Usage
snmp-server view *<1-128>* **mask** *<1-32 characters>* This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. **Command mode:** Global configuration
snmp-server view *<1-128>* **name** *<1-32 characters>* This command defines the name for a family of view subtrees. **Command mode:** Global configuration
snmp-server view *<1-128>* **tree** *<1-63 characters>* This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. **Command mode:** Global configuration
snmp-server view *<1-128>* **type {included|excluded}** This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` that define a family of view subtrees are included in or excluded from the MIB view. **Command mode:** Global configuration
no snmp-server view *<1-128>* Deletes the `vacmViewTreeFamily` group entry. **Command mode:** Global configuration
show snmp-server v3 view *<1-128>* Displays the current `vacmViewTreeFamily` configuration. **Command mode:** All

View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Table 161. *View-based Access Control Model Options*

Command Syntax and Usage
snmp-server access *<1-32>* **level {noAuthNoPriv|authNoPriv| |authPriv}** Defines the minimum level of security required to gain access rights. o `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. o `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. o `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
snmp-server access *<1-32>* **name** *<1-32 characters>* Defines the name of the group. **Command mode:** Global configuration
snmp-server access *<1-32>* **notify-view** *<1-32 characters>* Defines a notify view name that allows you notify access to the MIB view. **Command mode:** Global configuration
snmp-server access *<1-32>* **read-view** *<1-32 characters>* Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode:** Global configuration
snmp-server access *<1-32>* **security {usm|snmpv1|snmpv2}** Allows you to select the security model to be used. **Command mode:** Global configuration
snmp-server access *<1-32>* **write-view** *<1-32 characters>* Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode:** Global configuration

Table 161. *View-based Access Control Model Options (continued)*

Command Syntax and Usage
no snmp-server access *<1-32>* Deletes the View-based Access Control entry. **Command mode:** Global configuration
show snmp-server v3 access *<1-32>* Displays the View-based Access Control configuration. **Command mode:** All

SNMPv3 Group Configuration

The following table describes the SNMPv3 Group commands.

Table 162. *SNMPv3 Group Configuration Options*

Command Syntax and Usage
snmp-server group *<1-17>* **group-name** *<1-32 characters>* The name for the access group as defined in the following command: **snmp-server access** *<1-32>* **name** *<1-32 characters>* on page 383. **Command mode:** Global configuration
snmp-server group *<1-17>* **security {usm|snmpv1|snmpv2}** Defines the security model. **Command mode:** Global configuration
snmp-server group *<1-17>* **user-name** *<1-32 characters>* Sets the user name as defined in the following command: **snmp-server user** *<1-17>* **name** *<1-32 characters>* on page 383. **Command mode:** Global configuration
no snmp-server group *<1-17>* Deletes the `vacmSecurityToGroup` entry. **Command mode:** Global configuration
show snmp-server v3 group *<1-17>* Displays the current `vacmSecurityToGroup` configuration. **Command mode:** All

SNMPv3 Community Table Configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

Table 163. *SNMPv3 Community Table Configuration Options*

Command Syntax and Usage
snmp-server community *<1-16>* **index** *<1-32 characters>* Allows you to configure the unique index value of a row in this table. **Command string:** Global configuration
snmp-server community *<1-16>* **name** *<1-32 characters>* Defines the user name as defined in the following command: **snmp-server user** *<1-17>* **name** *<1-32 characters>* on page 383. **Command string:** Global configuration
snmp-server community *<1-16>* **tag** *<1-255 characters>* Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** Global configuration
snmp-server community *<1-16>* **user-name** *<1-32 characters>* Defines a readable string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
no snmp-server community *<1-16>* Deletes the community table entry. **Command mode:** Global configuration
show snmp-server v3 community *<1-16>* Displays the community table configuration. **Command mode:** All

SNMPv3 Target Address Table Configuration

These commands are used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

Table 164. *Target Address Table Configuration Options*

Command Syntax and Usage
snmp-server target-address *<1-16>* **address** *<IP address>* **name** *<1-32 characters>* Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **address6** *<IPv6 address>* **name** *<1-32 characters>* Allows you to configure the locally arbitrary, but unique identifier, target IPv6 address name associated with this entry. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **name** *<1-32 characters>* **address** *<transport IP address>* Configures a transport IPv4 address that can be used in the generation of SNMP traps. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **name** *<1-32 characters>* **address6** *<transport IPv6 address>* Configures a transport IPv6 address that can be used in the generation of SNMP traps. IPv6 addresses are not displayed in the configuration, but they do receive traps. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **parameters-name** *<1-32 characters>* Defines the name as defined in the following command: **snmp-server target-parameters** *<1-16>* **name** *<1-32 characters>* on page 389. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **port** *<TCP port range (1-65535)>* Allows you to configure a transport address port that can be used in the generation of SNMP traps. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **taglist** *<1-255 characters>* Allows you to configure a list of tags that are used to select target addresses for a particular operation. **Command mode:** Global configuration

Table 164. *Target Address Table Configuration Options (continued)*

Command Syntax and Usage
no snmp-server target-address *<1-16>* Deletes the Target Address Table entry. **Command mode:** Global configuration
show snmp-server v3 target-address *<1-16>* Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name and the security level (`noAuthnoPriv, authNoPriv` or `authPriv`).

Table 165. *Target Parameters Table Configuration Options*

Command Syntax and Usage
snmp-server target-parameters *<1-16>* **level {noAuthNoPriv| |authNoPriv|authPriv}** Allows you to select the level of security to be used when generating the SNMP messages using this entry. o `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. o `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. o `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
snmp-server target-parameters *<1-16>* **message {snmpv1|snmpv2c| |snmpv3}** Allows you to configure the message processing model that is used to generate SNMP messages. **Command mode:** Global configuration
snmp-server target-parameters *<1-16>* **name** *<1-32 characters>* Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry. **Command mode:** Global configuration

Table 165. *Target Parameters Table Configuration Options (continued)*

Command Syntax and Usage
snmp-server target-parameters *<1-16>* **security {usm|snmpv1| |snmpv2}** Allows you to select the security model to be used when generating the SNMP messages. **Command mode:** Global configuration
snmp-server target-parameters *<1-16>* **user-name** *<1-32 characters>* Defines the name that identifies the user in the USM table (page 383) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration
no snmp-server target-parameters *<1-16>* Deletes the `targetParamsTable` entry. **Command mode:** Global configuration
show snmp-server v3 target-parameters *<1-16>* Displays the current `targetParamsTable` configuration. **Command mode:** All

SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions and generates Notification-Class messages based on these events or conditions.

Table 166. *Notify Table Options*

Command Syntax and Usage
snmp-server notify *<1-16>* **name** *<1-32 characters>* Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry. **Command mode:** Global configuration
snmp-server notify *<1-16>* **tag** *<1-255 characters>* Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected. **Command mode:** Global configuration
no snmp-server notify *<1-16>* Deletes the notify table entry. **Command mode:** Global configuration
show snmp-server v3 notify *<1-16>* Displays the current notify table configuration. **Command mode:** All

System Access Configuration

The following table describes the System Access commands.

Table 167. *System Access Configuration Options*

Command Syntax and Usage
`[no] access http enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. The default settings is `enabled`. **Command mode:** Global configuration
`access http port` *<TCP port number (1-65535)>* Sets the switch port used for serving switch Web content. The default is HTTP port `80`. **Command mode:** Global configuration
`default access http port` Resets the HTTP port to the default port number - `80`. **Command mode:** Global configuration
`access snmp {read-only|read-write}` Enables read-only/write-read SNMP access. **Command mode:** Global configuration
`no access snmp` Disables SNMP access. **Command mode:** Global configuration
`[no] access telnet enable` Enables or disables Telnet access. The default setting is `enabled`. **Command mode:** Global configuration
`access telnet port` *<TCP port number (1-65535)>* Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port. **Command mode:** Global configuration
`default access telnet port` Resets the Telnet server port to the default port number - `23`. **Command mode:** Global configuration
`access tftp-port` *<TCP port number (1-65535)>* Sets the TFTP port for the switch. The default is port `69`. **Command mode:** Global configuration

Table 167. *System Access Configuration Options (continued)*

Command Syntax and Usage
default access tftp-port Resets the TFTP port to the default port number - 69. **Command mode:** Global configuration
[no] access tsbbi enable Enables or disables Telnet/SSH configuration through the Browser-Based Interface (BBI). **Command mode:** Global configuration
[no] access userbbi enable Enables or disables user configuration access through the Browser-Based Interface (BBI). **Command mode:** Global configuration
show access Displays the current system access parameters. **Command mode:** All

Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

Table 168. *Management Network Configuration Options*

Command Syntax and Usage
[no] access management-network *<mgmt network IPv4 address> <mgmt network IPv4 netmask>* Adds or removes a defined network through which switch access is allowed via Telnet, SNMP or the Enterprise NOS browser-based interface. A range of IPv4 addresses is produced when used with a network mask address. Specify an IPv4 address and mask address in dotted-decimal notation **Note**: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a "Network Down" state on the network. **Command mode:** Global configuration
[no] access management-network *<mgmt network IPv4 address> <mgmt network IPv4 netmask>* **{snmp-ro|snmp-rw}** Adds or removes a defined IPv4 network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IPv4 address and mask address in dotted-decimal notation. **Command mode:** Global configuration

Table 168. *Management Network Configuration Options*

Command Syntax and Usage
no access management-network {snmp-ro|snmp-rw} Clears the IPv4 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
[no] access management-network6 *<mgmt network IPv6 address> <IPv6 prefix length>* Adds or removes a defined network through which switch access is allowed via Telnet, SNMP or the Enterprise NOS browser-based interface. A range of IPv6 addresses is produced when used with a prefix length. Specify an IPv6 address in hexadecimal format with colons. **Note:** If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a "Network Down" state on the network. **Command mode:** Global configuration
[no] access management-network6 *<mgmt network IPv6 address> <IPv6 prefix length>* **{snmp-ro|snmp-rw}** Adds or removes a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed. **Command mode:** Global configuration
no access management-network6 {snmp-ro|snmp-rw} Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
show access management-network Displays the current management network configuration. **Command mode:** Privileged EXEC
clear access management-network Removes all defined management networks. **Command mode:** Privileged EXEC

NETCONF Configuration

This menu allows you to configure support for Network Configuration Protocol (NETCONF), which provides mechanisms to install, manipulate and delete the configuration of network devices. NETCONF is described in RFC 4741.

Table 169. *NETCONF Configuration Options*

Command Syntax and Usage
`[no] access netconf enable` Enables or disables NETCONF access to the switch. **Command mode:** Global configuration
`access netconf timeout` *<30-3600>* Configures the timeout value for NETCONF sessions, in seconds. The default value is `300` seconds. **Command mode:** Global configuration
`default access netconf timeout` Resets the timeout value for NETCONF sessions to the default of `300` seconds. **Command mode:** Global configuration
`show access` Displays the current configuration. **Command mode:** All

NETCONF over SSH Configuration

This menu allows you to enable NETCONF access over Secure Shell (SSH). NETCONF over SSH is described in RFC 4742.

Table 170. *NETCONF over SSH Configuration Options*

Command Syntax and Usage
`[no] access netconf ssh enable` Enables or disables NETCONF access over SSH. **Command mode:** Global configuration
`access netconf ssh port` *<TCP port number (1-65535)>* Configures the TCP port used for NETCONF. The default port number is `830`. **Command mode:** Global configuration
`default netconf ssh port` Resets the SSH port used for NETCONF to the default port number - `830`. **Command mode:** Global configuration

User Access Control Configuration

The following table describes user-access control commands.

Note: Passwords can be a maximum of 64 characters.

Table 171. *User Access Control Configuration Options*

Command Syntax and Usage
access user *<1-20>* Configures the User ID. For more command options, see page 396. **Command mode:** Global configuration
[no] access user administrator-enable Enables or disables the default administrator account. **Command mode:** Global configuration
access user administrator-password Sets the administrator (admin) password. The administrator has complete access to all menus, information and configuration commands on the G8272, including the ability to change both the user and administrator passwords. This command will prompt for required information: current admin password, new password (up to 64 characters) and confirmation of the new password. Access includes "oper" functions. **Note:** You cannot disable the administrator password. **Command Mode**: Global configuration
access user eject {*<user name>***|session-id** *<session ID>***}** Ejects the specified user from the G8272. **Command mode:** Global configuration
access user operator-password Sets the operator (oper)password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports. This command will prompt for required information: current admin password, new password (up to 64 characters) and confirmation of the new password. **Note:** To disable the operator account, set the password to null (no password). The default setting is disabled (no password). **Command Mode**: Global configuration
access user user-password Sets the user (user) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes. This command will prompt for required information: current admin password, new password (up to 64 characters) and confirmation of the new password. **Note:** To disable the user account, set the password to null (no password). **Command Mode**: Global configuration

Table 171. *User Access Control Configuration Options*

Command Syntax and Usage
show access user Displays the current user status. **Command mode:** Privileged EXEC
clear line *<1-12>* Ejects the user with the corresponding session ID from the G8272. **Command mode:** Privileged EXEC

System User ID Configuration

The following table describes the System User ID commands.

Table 172. *User ID Configuration Options*

Command Syntax and Usage
[no] access user *<1-20>* **enable** Enables or disables the user ID. **Command mode:** Global configuration
access user *<1-20>* **level {user|operator|administrator}** Sets the Class-of-Service to define the user's authority level. Enterprise NOS defines these levels as: User, Operator and Administrator, with User being the most restricted level. **Command mode:** Global configuration
access user *<1-20>* **name** *<1-64 characters>* Defines the user name of maximum eight characters. **Command mode:** Global configuration
access user *<1-20>* **password** Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 64 characters) and confirmation of the new password. **Command mode:** Global configuration
no access user *<1-20>* Deletes the user ID. **Command mode:** Global configuration
show access user Displays the current user ID configuration. **Command mode:** Privileged EXEC

Strong Password Configuration

The following table describes the Strong Password commands.

Table 173. *Strong Password Configuration Options*

Command Syntax and Usage
access user strong-password clear local user {lockout|fail-attempts} {<*username*>**|all}** Enables locked out accounts or resets failed login counters for all users or for a specific user. **Command mode:** Global configuration
[no] access user strong-password enable Enables or disables Strong Password requirement. **Command mode:** Global configuration
access user strong-password expiry <1-365> Configures the number of days allowed before the password must be changed. The default value is `60` days. **Command mode:** Global configuration
access user strong-password faillock <1-10> Configures the number of failed login attempts that trigger the account lockout. The default value is `6` attempts. **Command mode:** Global configuration
access user strong-password faillog <1-255> Configures the number of failed login attempts allowed before a security notification is logged. The default value is `3` login attempts. **Command mode:** Global configuration
[no] access user strong-password lockout Enables or disables account lockout after a specified number of failed login attempts. The default setting is `disabled`. **Command mode:** Global configuration

Table 173. *Strong Password Configuration Options*

Command Syntax and Usage
access user strong-password warning *<1-365>* Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days. **Command mode:** Global configuration
show access user strong-password Displays the current Strong Password configuration. **Command mode:** Privileged EXEC

HTTPS Access Configuration

The following table describes the HTTP Access commands.

Table 174. *HTTPS Access Configuration Options*

Command Syntax and Usage
[no] access https enable Enables or disables BBI access (Web access) using HTTPS. **Command mode:** Global configuration
access https generate-certificate Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: o Country Name (2 letter code): CA o State or Province Name (full name): Ontario o Locality Name (for example, city): Ottawa o Organization Name (for example, company): Lenovo o Organizational Unit Name (for example, section): Operations o Common Name (for example, user's name): Mr Smith o Email (for example, email address): info@lenovo.com You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent. **Command mode:** Global configuration

Table 174. *HTTPS Access Configuration Options (continued)*

Command Syntax and Usage
access https generate-csr Allows you to generate a CSR (Certificate Signing Request) to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: o Country Name (2 letter code): CA o State or Province Name (full name): Ontario o Locality Name (for example, city): Ottawa o Organization Name (for example, company): Lenovo o Organizational Unit Name (for example, section): Operations o Common Name (for example, user's name): Mr Smith o Email (for example, email address): info@lenovo.com Unlike the **generate-certificate** command, this command will generate a certificate request that needs to be signed by a certificate authority (CA) recognized by both parties. **Command mode:** Global configuration
access https save-certificate Allows the client or the Web browser to accept the certificate and save the certificate to Flash to be used when the switch is rebooted. **Command mode:** Global configuration
access https delete-certificate Deletes the current certificate from the flash memory. **Command mode:** Global configuration
access https port *<TCP port number (1-65535)>* Defines the HTTPS Web server port number. The default port is 443. **Command mode:** Global configuration
default access https port Resets the HTTPS port to the default port number - 443. **Command mode:** Global configuration
copy {tftp|sftp} ca-cert [data-port|mgt-port] Enables you to import a certificate authority root certificate using TFTP/SFTP. **Command mode:** Global configuration
copy tftp ca-cert address *<hostname or server IP address>* **filename** *<server-filename>* **[data-port|mgt-port]** Enables you to import a certificate authority root certificate using TFTP. **Command mode:** Global configuration

Table 174. *HTTPS Access Configuration Options (continued)*

Command Syntax and Usage
copy {tftp|sftp} host-cert [data-port|mgt-port] Enables you to import a host certificate using TFTP/SFTP. **Command mode:** Global configuration
copy tftp host-cert address *<hostname or server IP address>* **filename** *<server-filename>* **[data-port|mgt-port]** Enables you to import a host certificate using TFTP. **Command mode:** Global configuration
copy {tftp|sftp} host-key [data-port|mgt-port] Enables you to import a host private key using TFTP/SFTP. **Command mode:** Global configuration
copy tftp host-key address *<hostname or server IP address>* **filename** *<server-filename>* **[data-port|mgt-port]** Enables you to import a host private key using TFTP. **Command mode:** Global configuration
copy {tftp|sftp} public-key [data-port|mgt-port] Enables you to import a client public key using TFTP/SFTP. **Command mode:** Global configuration
copy tftp public-key address *<hostname or server IP address>* **filename** *<server-filename>* **[data-port|mgt-port]** Enables you to import a client public key using TFTP. **Command mode:** Global configuration
copy cert-request {tftp|ftp|sftp} address *<hostname or server IP address>* **filename** *<server-filename>* **[data-port|mgt-port]** Enables you to export a CSR to an external server using TFTP/SFTP/FTP. **Command mode:** Global configuration
show https host-csr pem-format Displays the generated CSR in PEM format. **Command mode:** Privileged EXEC
show https host-csr txt-format Displays the generated CSR in TXT format. **Command mode:** Privileged EXEC
show access Displays the current SSL Web Access configuration. **Command mode:** Privileged EXEC

Custom Daylight Saving Time Configuration

Use these commands to configure custom Daylight Saving Time. The DST is defined by two rules, the start rule and end rule. The rules specify the dates when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:
2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:
0070901 = September 7, at 1:00 a.m.

Table 175. *Custom DST Options*

Command Syntax and Usage
[no] system custom-dst enable Enables or disables the Custom Daylight Saving Time settings. **Command mode:** Global configuration
system custom-dst start-rule <*WDDMMhh*> Configures the start date for custom DST, as follows: WDMMhh W = week (0-5, where 0 means use the calendar date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23) **Note**: Week 5 is always considered to be the last week of the month. **Command mode:** Global configuration
system custom-dst end-rule <*WDDMMhh*> Configures the end date for custom DST, as follows: WDMMhh W = week (0-5, where 0 means use the calendar date) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) hh = hour (0-23) **Note**: Week 5 is always considered to be the last week of the month. **Command mode:** Global configuration
show custom-dst Displays the current Custom DST configuration. **Command mode:** All

sFlow Configuration

Enterprise NOS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

Table 176. *sFlow Configuration Options*

Command Syntax and Usage
`[no] sflow enable` Enables or disables the sFlow agent. **Command mode:** Global configuration
`sflow port` *<UDP port number (1-65000)>* Configures the UDP port for the sFlow server. The default value is `6343`. **Command mode:** Global configuration
`default sflow port` Resets the sFlow server port to the default port number - `6343`. **Command mode:** Global configuration
`sflow server` *<IP address>* **`[data-port|mgt-port]`** Defines the sFlow server address and interface port. **Command mode:** Global configuration
`no sflow server` Deletes the sFlow server address. **Command mode:** Global configuration.
`show sflow` Displays sFlow configuration parameters. **Command mode:** All

sFlow Port Configuration

Use the following commands to configure the sFlow port on the switch.

Table 177. *sFlow Port Configuration Options*

Command Syntax and Usage
sflow polling *<5-60>* Configures the sFlow polling interval, in seconds. The default setting is `disabled`. **Command mode:** Interface port
no sflow polling Disables sFlow polling interval. **Command mode:** Interface port
sflow sampling *<256-65536>* Configures the sFlow sampling rate, in packets per sample. The default setting is `disabled`. **Command mode:** Interface port
no sflow sampling Disables sFlow sampling rate. **Command mode:** Interface port

Server Port Configuration

Use these commands to define a list of server ports. Ports that are not configured as server ports are considered to be uplink ports. VMready learns Virtual Machine information only from server ports.

Table 178. *Server Port Configuration Options*

Command Syntax and Usage
`[no] system server-ports port` *<port alias or number>* Adds or removes one or more ports to the list of server ports. **Command mode:** Global configuration
`show system server-ports` Displays the current server port configuration. **Command mode:** All

Port Configuration

Use the Port Configuration commands to configure settings for interface ports.

Table 179. *Port Configuration Options*

Command Syntax and Usage
`interface port` *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
`interface portchannel {`*<1-72>***`|`***<73-144>***`|lacp`** *<1-65535>***`}`** Enter Interface portchannel mode. These commands allow you to configure port parameters for all port members in the selected Link Aggregation Group (LAG). **Command mode:** Global configuration
`[no] openflow mgmtport` *<port alias or number>* Enables or disables OpenFlow management state for the ports. **Note:** Supported in OpenFlow Only mode. **Command mode**: Global Configuration
`[no] bpdu-guard` Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports configured as `edge` ports. **Command mode:** Interface port/Interface portchannel
`description` *<1-64 characters>* Sets a description for the port. The assigned port description appears next to the port number on some information and statistics screens. The default is set to the port number. **Command mode:** Interface port/Interface portchannel
`no description` Removes the interface description. **Command mode:** Interface port/Interface portchannel
`dot1p` *<0-7>* Configures the port's 802.1p priority level. **Command mode:** Interface port/Interface portchannel
`dot1x` Configures 802.1X port-based authentication. For more command options, see page 455. **Command mode:** Interface port

Table 179. *Port Configuration Options (continued)*

Command Syntax and Usage
`[no] dscp-marking` Enables or disables DSCP re-marking on a port. **Command mode:** Interface port/Interface portchannel
`[no] flood-blocking` Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port. **Command mode:** Interface port/Interface portchannel
`ip dhcp snooping limit rate` *<1-2048>* Configures the maximum number of DHCP packets allowed per second. **Command mode:** Interface port
`no ip dhcp snooping limit rate` Unlimits the maximum number of DHCP packets allowed per second. **Command mode:** Interface port
`[no] ip dhcp snooping trust` Configures this port as a trusted port for DHCP packets from the server. **Command mode:** Interface port
`[no] learning` Enables or disables FDB learning on the port. **Command mode:** Interface port/Interface portchannel
`[no] mac-address-table mac-notification` Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table. **Command mode:** Interface port/Interface portchannel
`port-channel min-links` *<1-32>* Set the minimum number of links for the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the Link Aggregation Group (LAG) is placed in the `down` state. **Command mode:** Interface port
`[no] ptp` Enables or disables PTP on the current port. Disabled ports will not support PTP even if PTP is globally enabled. The default setting is `enabled`. **Note:** PTP is not supported on management ports. **Command mode**: Interface port/Interface portchannel

Table 179. *Port Configuration Options (continued)*

Command Syntax and Usage
`[no] reflective-relay force` Enables or disables constraint to always keep reflective relay active. The default setting is `disabled`. **Command mode:** Interface port
`[no] rmon` Enables or disables Remote Monitoring (RMON) on the current port. **Command mode:** Interface port/Interface portchannel
`shutdown` Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 413.) **Command mode:** Interface port/Interface portchannel
`no shutdown` Enables the port. **Command mode:** Interface port/Interface portchannel
`storm-control {broadcast|multicast|unicast} level rate` *<0-2097151>* Limits the available bandwidth for broadcast, multicast or unicast messages to the specified value. **Command mode:** Interface port/Interface portchannel
`no storm-control {broadcast|multicast|unicast}` Sets the port to forward all broadcast, multicast or unicast packets. **Command mode:** Interface port/Interface portchannel
`[no] switchport` Enables or disables routing on a port. **Command mode:** Interface port/Interface portchannel
`switchport access vlan` *<VLAN ID (1-4094)>* Configures the associated VLAN used in access mode. Default value is `1` for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel
`no switchport access vlan` Resets the access VLAN to its default value. **Command mode:** Interface port/Interface portchannel

Table 179. *Port Configuration Options (continued)*

Command Syntax and Usage
`switchport mode {access|trunk|private-vlan}` Configures the port's trunking mode: o `access` allows association to a single VLAN o `trunk` automatically adds the port to all created VLANs. To configure a specific allowed VLAN range for the port use the command: **`switchport trunk allowed vlan`** o `private-vlan` allows association to a private VLAN Default mode is `access`. **Note**: When switching from access to trunk mode, the port inherits the access VLAN as the trunk Native-VLAN. **Note**: When switching from trunk to access mode, the port inherits the trunk Native-VLAN as the access VLAN. **Command mode:** Interface port/Interface portchannel
`no switchport mode private-vlan` Removes private-VLAN mode from the port. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan host-association` *<primary VLAN ID (2-4094)> <secondary VLAN ID (2-4094)>* Enables or disables the private VLAN association on a secondary port. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan mapping` *<primary VLAN ID (2-4094)>* Enables or disables private VLAN mapping on a port in promiscuous mode. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan` *<VLAN ID (1-4094)>* Configures the allowed VLANs in trunk mode for the current port or portchannel. If the allowed range does not have any existing VLANs, the lowest-numbered VLAN is created and becomes the Native-VLAN. If the allowed range contains an existing VLAN(s), but the Native-VLAN is not in the allowed range, the Native-VLAN is changed to the lowest-numbered existing VLAN. If a new VLAN is created and it is part of the allowed VLAN range, the port will also be added to that VLAN. **Command mode:** Interface port/Interface portchannel

Table 179. *Port Configuration Options (continued)*

Command Syntax and Usage
`switchport trunk allowed vlan {add|remove}` *<VLAN ID (1-4094)>* Updates the associated VLANs in trunk mode. o `add` enables the VLAN range in addition to the current configuration. If any VLAN in the range does not exist, it will not be created and enabled automatically. If a new VLAN is created and it is part of the allowed VLAN range, the port will also be added to that VLAN. o `remove` eliminates the VLAN range from the current configuration. If the Native-VLAN is in the specified range, the smallest available VLAN from the remaining range will become the new Native-VLAN. If the remaining range does not have any existing VLANs, the lowest-numbered VLAN is created and becomes the Native-VLAN. **Note:** The remaining VLAN range must contain at least one VLAN. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {all|none}` Updates the associated VLANs in trunk mode. o `all` associates the port to all existing regular VLANs and to any other VLAN that gets created afterwards. o `none` removes the port from all currently associated VLANs and assigns the port to the default VLAN (`VLAN 1` for data ports and `VLAN 4095` for the management port). **Command mode:** Interface port/Interface portchannel
`no switchport trunk allowed vlan` Assigns the port to all available data VLANs. **Command mode:** Interface port/Interface portchannel
`switchport trunk native vlan` *<VLAN ID (1-4094)>* Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it is automatically created. The VLAN must be present in the port's allowed VLAN range. The default value is `1` for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel
`[no] tagpvid-ingress` Enables or disables tagging the ingress frames with the port's VLAN ID. When enabled, the Native VLAN (PVID) tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID. The default setting is `disabled`. **Command mode**: Interface port/Interface portchannel

Table 179. *Port Configuration Options (continued)*

Command Syntax and Usage
`[no] tagskip-egress` Enables or disables egress VLAN tag enforcement to be skipped. **Note**: STP must be globally disabled on the switch and all VLANs must be assigned to the default STG. **Command mode**: Interface port/Interface portchannel
`[no] tagskip-ingress` Enables or disables ingress VLAN tag enforcement to be skipped. **Command mode**: Interface port/Interface portchannel
`[no] vlan dot1q tag native` Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is `disabled`. **Note:** In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterwords. Also, as an operational command, it will not be dumped into the configuration file. **Command mode:** Global configuration/Interface port/Interface portchannel
`show interface port` *<port alias or number>* Displays the specified port's parameters. **Command mode:** All

Port Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 180. *Port Error Disable Options*

Command Syntax and Usage
`[no] errdisable recovery` Enables or disables automatic error-recovery for the port. The default setting is `enabled`. **Note**: Error-recovery must be enabled globally before port-level commands become active. **Command mode:** Interface port/Interface portchannel
`show interface port` *<port alias or number>* **`errdisable`** Displays the specified port's Error Disable parameters. **Command mode:** All

Port Link Flap Dampening Configuration

The following table describes the Port Link Flap Dampening commands.

Table 181. *Port Link Flap Dampening Configuration Options*

Command Syntax and Usage
`[no] errdisable link-flap enable` Enables or disables Link Flap Dampening on the port. For more information, see "Link Flap Dampening Configuration" on page 353. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`errdisable link-flap`** Displays the current Link Flap Dampening parameters for the specified port. **Command mode:** All

Port Link Configuration

Use these commands to configure link-level parameters for the port/portchannel.

Table 182. *Port Link Configuration Options*

Command Syntax and Usage
`[no] auto` Enables or disables auto-negotiation. **Note**: Data ports are fixed at 10000 Mbps, and cannot be set to auto-negotiate, unless a 1 Gb SFP transceiver is used. **Command mode:** Interface port/Interface portchannel
`duplex {full|half|auto}` Sets the operating mode. The choices include: o Auto negotiation (default) o Half-duplex o Full-duplex **Note**: Data ports are fixed at full duplex. **Command mode:** Interface port/Interface portchannel
`flowcontrol {receive|send} {on|off}` Turns flow control receiving or transmiting on or off. **Command mode:** Interface port/Interface portchannel
`no flowcontrol` Disables flow control on the current port. **Command mode:** Interface port/Interface portchannel
`show interface port` *<port alias or number>* Displays the specified port's parameters. **Command mode:** All

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
RS G8272(config)# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the RackSwitch G8272 is rebooted. See the "Operations Commands" on page 687 for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 183. *Port UDLD Configuration Options*

Command Syntax and Usage
`[no] udld` Enables or disables UDLD on the port. **Command mode:** Interface port
`[no] udld aggressive` Configures the UDLD mode for the selected port, as follows: o **Normal**: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the "no" form to select normal operation. o **Aggressive**: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`udld`** Displays the specified port's UDLD parameters. **Command mode:** All

Port OAM Configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard. OAM Discovery commands are described in the following table.

Table 184. *Port OAM Configuration Options*

Command Syntax and Usage
[no] oam Enables or disables OAM discovery on the current port. **Command mode:** Interface port
[no] oam passive Enables or disables OAM discovery passive mode. In passive mode, the current port allows its peer link to initiate OAM discovery. If OAM determines that the port is in an anomalous condition, the port is disabled. **Command mode:** Interface port
show interface port *<port alias or number>* **oam** Displays the specified port's OAM parameters. **Command mode:** All

Port ACL Configuration

The following table describes the Port ACL commands.

Table 185. *Port ACL Configuration Options*

Command Syntax and Usage
`[no] access-control group` *<1-256>* Adds or removes the specified ACL group to the port. You can add multiple ACL groups to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port/Interface portchannel
`[no] access-control list` *<1-256>* Adds or removes the specified ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port/Interface portchannel
`[no] access-control list6` *<1-128>* Adds or removes the specified IPv6 ACL to the port. You can add multiple ACLs to a port, but the total number of precedence levels allowed is two. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`access-control`** Displays current ACL QoS parameters. **Command mode:** All

Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see "Weighted Random Early Detection Configuration" on page 423.

Table 186. *Port WRED Options*

Command Syntax and Usage
`[no] random-detect enable` Enables or disables Random Detection and avoidance. **Command mode:** Interface port
`[no] random-detect ecn enable` Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions. **Note**: ECN functions only on TCP traffic. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`random-detect`** Displays current Random Detection and avoidance parameters. **Command mode:** All

Port WRED Transmit Queue Configuration

Use this menu to define WRED thresholds for the port's transmit queues. Set each threshold between 1% and 100%. When the average queue size grows beyond the minimum threshold, packets begin to be dropped. When the average queue size reaches the maximum threshold, all packets are dropped. The probability of packet-drop between the thresholds is defined by the drop rate.

Table 187. *Port WRED Transmit Queue Options*

Command Syntax and Usage
[no] random-detect transmit-queue *<0-7>* **enable** Enables or disables the WRED transmit queue configuration. **Command mode:** Interface port
random-detect transmit-queue *<0-7>* **tcp min-threshold** *<1-100>* **max-threshold** *<1-100>* **drop-rate** *<1-100>* Configures the WRED thresholds for TCP traffic. **Command mode:** Interface port
no random-detect transmit-queue *<0-7>* **tcp** Clears the WRED configuration for TCP traffic. **Command mode:** Interface port
random-detect transmit-queue *<0-7>* **non-tcp min-threshold** *<1-100>* **max-threshold** *<1-100>* **drop-rate** *<1-100>* Configures the WRED thresholds for non-TCP traffic. **Command mode:** Interface port
no random-detect transmit-queue *<0-7>* **non-tcp** Clears the WRED configuration for non-TCP traffic. **Command mode:** Interface port

Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

802.1p Configuration

This feature provides the G8272 the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 188. *802.1p Configuration Options*

Command Syntax and Usage
qos transmit-queue mapping *<priority (0-7)> <COSq number (0-7)>* Maps the 802.1p priority to the Class of Service queue (COSq) priority. Enter the 802.1p priority value, followed by the Class of Service queue that handles the matching traffic. **Command mode:** Global configuration
default qos transmit-queue mapping Resets the 802.1p packet priority mapping to its default values. **Command mode:** Global configuration
qos transmit-queue weight-cos *<COSq number (0-7)> <weight (0-15)>* Configures the weight of the selected Class of Service queue (COSq). Enter the queue number, followed by the scheduling weight. **Command mode:** Global configuration
default qos transmit-queue weight Resets the weights of Class of Service queues to their default values. **Command mode:** Global configuration
show qos transmit-queue Displays the current 802.1p parameters. **Command mode:** All

DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to a new value or to an 802.1p priority value.

Table 189. *DSCP Configuration Options*

Command Syntax and Usage
qos dscp dot1p-mapping *<DSCP (0-63)> <priority (0-7)>* Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value. **Command mode:** Global configuration
qos dscp dscp-mapping *<DSCP (0-63)> <new DSCP (0-63)>* Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value of incoming packets, followed by the new value. **Command mode:** Global configuration
[no] qos dscp re-marking Globally enables or disables DSCP re-marking. **Command mode:** Global configuration
show qos dscp Displays the current DSCP parameters. **Command mode:** All

Control Plane Protection

These commands allow you to limit the number of selected protocol packets received by the control plane (CP) of the switch. These limits help protect the CP from receiving too many protocol packets in a given time period.

Table 190. *Control Plane Protection Options*

Command Syntax and Usage
`qos protocol-packet-control packet-queue-map` *<packet queue number (0-43)> <packet type>* Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed: o `802.1x` (IEEE 802.1x packets) o `application-cri-packets` (critical packets of applications) o `arp-bcast` (ARP broadcast packets) o `arp-ucast` (ARP unicast reply packets) o `bgp` (BGP packets) o `bpdu` (Spanning Tree Protocol packets) o `cisco-bpdu` (Cisco STP packets) o `dest-unknown` (packets with destination not yet learned) o `dhcp` (DHCP packets) o `ecp` (ECP packets) o `fips` (FIPS packets) o `icmp` (ICMP packets) o `icmp6` (ICMP6 packets) o `igmp` (IGMP packets) o `ipv4-miscellaneous` (IPv4 packets with IP options and TTL exception) o `ipv6-nd` (IPv6 Neighbor Discovery packets) o `lacp` (LACP/Link Aggregation protocol packets) o `lldp` (LLDP packets) o `oflow-cntrler` (Packets hit OpenFlow send-to-controller filter) o `oflow-default` (Packets hit OpenFlow default filter) o `oflow-mgmt` (Packets hit OpenFlow management filter) o `ospf` (OSPF packets) o `ospf3` (OSPF3 Packets) o `pim` (PIM packets) o `ptp` (PTP packets) o `rip` (RIP packets) o `system` (system protocols, such as tftp, ftp, telnet, ssh) o `udld` (UDLD packets) o `vlag` (VLAG packets) o `vrrp` (VRRP packets) **Command mode:** Global configuration

Table 190. *Control Plane Protection Options (continued)*

Command Syntax and Usage
no qos protocol-packet-control packet-queue-map *<packet type>* Clears the selected packet type from its associated packet queue. **Command mode:** Global configuration
qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-43)> <1-10000>* Configures the number of packets per second allowed for each packet queue. **Command mode:** Global configuration
no qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-43)>* Clears the packet rate configured for the selected packet queue. **Command mode:** Global configuration
show qos protocol-packet-control information protocol Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. **Command mode:** All
show qos protocol-packet-control information queue Displays the packet rate configured for each packet queue. **Command mode:** All

Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. The G8272 implementation of WRED defines TCP and non-TCP traffic profiles on a per-port, per COS queue basis. For each port, you can define a transmit-queue profile with thresholds that define packet-drop probability.

These commands allow you to configure global WRED parameters. For port WRED commands, see "Port WRED Configuration" on page 417.

Table 191. *WRED Configuration Options*

Command Syntax and Usage
`[no] qos random-detect ecn enable` Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions. **Note**: ECN functions only on TCP traffic. **Command mode:** Global configuration
`[no] qos random-detect enable` Enables or disables Random Detection and avoidance. **Command mode:** Global configuration
`show qos random-detect` Displays current Random Detection and avoidance parameters. **Command mode:** All

WRED Transmit Queue Configuration

The following table describes the WRED Transmit Queue commands.

Table 192. *WRED Transmit Queue Options*

Command Syntax and Usage
[no] qos random-detect transmit-queue *<0-7>* **enable** Enables or disables the WRED transmit queue configuration. **Command mode:** Global configuration
qos random-detect transmit-queue *<0-7>* **non-tcp min-threshold** *<min. threshold (1-100)>* **max-threshold** *<max. threshold (1-100)>* **drop-rate** *<drop rate (1-100)>* Configures the WRED thresholds for non-TCP traffic. **Command mode:** Global configuration
qos random-detect transmit-queue *<0-7>* **tcp min-threshold** *<min. threshold (1-100)>* **max-threshold** *<max. threshold (1-100)>* **drop-rate** *<drop rate (1-100)>* Configures the WRED thresholds for TCP traffic. **Command mode:** Global configuration
no qos random-detect transmit-queue *<0-7>* **{non-tcp|tcp}** Deletes the WRED configuration for non-TCP or TCP traffic. **Command mode:** Global configuration

Access Control Configuration

Use these commands to create Access Control Lists. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see "Port ACL Configuration" on page 416.

Table 193. *General ACL Configuration Options*

Command Syntax and Usage
access-control group *<1-256>* Configures an ACL Group. To view command options, see page 444. **Command mode:** Global configuration
access-control list *<1-256>* Configures an Access Control List. To view command options, see page 426. **Command mode:** Global configuration
access-control list6 *<1-128>* Configures an IPv6 Access Control List. To view command options, see page 436. **Command mode:** Global configuration
access-control macl *<1-256>* Configures an Access Control List. To view command options, see page 445. **Command mode:** Global configuration
access-control vmap *<1-128>* Configures an ACL VLAN map. To view command options, see page 448. **Command mode:** Global configuration
show access-control Displays the current ACL parameters. **Command mode:** All

Access Control List Configuration

These commands allow you to define filtering criteria for each Access Control List (ACL).

Table 194. *ACL Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **action {permit|deny| |set-priority** *<0-7>***}** Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets or set the 802.1p priority level. **Command mode:** Global configuration
access-control list *<1-256>* **action redirect {port** *<port number>***|portchannel** *<1-64>***}** Configures the redirection of packets that match the ACL definitions. You can choose to redirect packets either through an ethernet port or a Link Aggregation Group (LAG). **Command mode**: Global configuration
access-control list *<1-256>* **egress-port port** *<port alias or number>* Configures the ACL to function on egress packets. **Command mode:** Global configuration
no access-control list *<1-256>* **egress-port** Disables the ACL to function on egress packets. **Command mode:** Global configuration
[no] access-control list *<1-256>* **log** Enables or disables logging for the Access Control List. **Note**: Enabling the LOG feature neutralizes ACL deny filter actions for Telnet and SSH traffic that is addressed to the switch's Layer 3 interfaces. **Command mode:** Global configuration
[no] access-control list *<1-256>* **statistics** Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration
default access-control list *<1-256>* Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list *<1-256>* Displays the current ACL parameters. **Command mode:** All

ACL Mirroring Configuration

These commands allow you to define port mirroring for an ACL. Packets that match the ACL are mirrored to the destination interface.

Table 195. *ACL Port Mirroring Options*

Command Syntax and Usage
access-control list *<1-256>* **mirror port** *<port alias or number>* Configures the destination to which packets that match this ACL are mirrored. **Command mode:** Global configuration
no access-control list *<1-256>* **mirror** Removes all mirrored packets. **Command mode:** Global configuration
show access-control list *<1-256>* **mirror** Displays the current port mirroring parameters for the ACL. **Command mode:** All

Ethernet Filtering Configuration

These commands allow you to define Ethernet matching criteria for an ACL.

Table 196. *Ethernet Filtering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **ethernet destination-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the destination MAC address for this ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **ethernet destination-mac-address** Removes the destination MAC address for this ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ethernet ethernet-type {arp|ip|ipv6|mpls|rarp|any|***<other (0x600-0xFFFF)>***}** Defines the Ethernet type for this ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **ethernet ethernet-type** Removes the Ethernet type for this ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ethernet priority** *<0-7>* Defines the Ethernet priority value for the ACL. **Command mode:** Global configuration

Table 196. *Ethernet Filtering Configuration Options*

Command Syntax and Usage
no access-control list *<1-256>* **ethernet priority** Removes the Ethernet priority value for the ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ethernet source-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the source MAC address for this ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **ethernet source-mac-address** Removes the source MAC address for this ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ethernet vlan** *<VLAN ID (1-4094)>* **[***<VLAN mask>***]** Defines a VLAN number and mask for this ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **ethernet vlan** Removes VLAN number and mask for this ACL. **Command mode:** Global configuration
default access-control list *<1-256>* **ethernet** Resets Ethernet parameters for the ACL to their default values. **Command mode:** Global configuration
no access-control list *<1-256>* **ethernet** Removes Ethernet parameters for the ACL. **Command mode:** Global configuration
show access-control list *<1-256>* **ethernet** Displays the current Ethernet parameters for the ACL. **Command mode:** All

IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 197. *IP version 4 Filtering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **ipv4 destination-ip-address** *<IP address>* **[***<IP mask>***]** Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **ipv4 destination-ip-address** Deletes the configured destination IP address for the specified ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ipv4 protocol** *<0-255>* Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp **Command mode:** Global configuration
no access-control list *<1-256>* **ipv4 protocol** Deletes the configured IP protocol for the specified ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ipv4 source-ip-address** *<IP address>* **[***<IP mask>***]** Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation. **Command mode:** Global configuration
no access-control list *<1-256>* **ipv4 source-ip-address** Deletes the configured source IP address for the specified ACL. **Command mode:** Global configuration
access-control list *<1-256>* **ipv4 type-of-service** *<0-255>* Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349. **Command mode:** Global configuration

Table 197. *IP version 4 Filtering Configuration Options*

Command Syntax and Usage
no access-control list *<1-256>* **ipv4 type-of-service** Deletes the configured Type of Service (ToS) value for the specified ACL. **Command mode:** Global configuration
default access-control list *<1-256>* **ipv4** Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-256>* **ipv4** Displays the current IPv4 parameters. **Command mode:** All

TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 198. *TCP/UDP Filtering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **tcp-udp source-port** *<1-65535>* **[***<mask (0xFFFF)>***]** Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports: **Number** **Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
no access-control list *<1-256>* **tcp-udp source-port** Disables the configured source port for the specified ACL. **Command mode:** Global configuration

Table 198. *TCP/UDP Filtering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **tcp-udp destination-port** *<1-65535>* **[**<*mask (0xFFFF)*>**]** Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `source-port`. **Command mode:** Global configuration
no access-control list *<1-256>* **tcp-udp destination-port** Disables the configured destination port for the specified ACL. **Command mode:** Global configuration
access-control list *<1-256>* **tcp-udp flags** *<value (0x0-0x3f)>* **[**<*mask (0x0-0x3f)*>**]** Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **tcp-udp flags** Disables the configured TCP/UDP flag for the specified ACL. **Command mode:** Global configuration
default access-control list *<1-256>* **tcp-udp** Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-256>* **tcp-udp** Displays the current TCP/UDP Filtering parameters. **Command mode:** All

Packet Format Filtering Configuration

These commands allow you to define Packet Format matching criteria for an ACL.

Table 199. *Packet Format Filtering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **packet-format ethernet {ethertype2|snap|llc}** Defines the Ethernet format for the ACL. **Command mode:** Global configuration
access-control list *<1-256>* **packet-format ip {ipv4|ipv6}** Defines the IP format for the ACL. **Command mode:** Global configuration
access-control list *<1-256>* **packet-format tagging {any|none| |tagged}** Defines the tagging format for the ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **packet-format {ethernet|ip| |tagging}** Deletes the selected format for the specified ACL. **Command mode:** Global configuration
default access-control list *<1-256>* **packet-format** Resets Packet Format parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-256>* **packet-format** Displays the current Packet Format parameters for the ACL. **Command mode:** All

ACL Metering Configuration

These commands define the Access Control profile for the selected ACL.

Table 200. *ACL Metering Configuration Options*

Command Syntax and Usage
access-control list *<1-256>* **meter action {drop|pass}** Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control list *<1-256>* **meter committed-rate** *<64-40000000>* Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
[no] access-control list *<1-256>* **meter enable** Enables or disables ACL Metering. **Command mode:** Global configuration
access-control list *<1-256>* **meter maximum-burst-size** *<32-4096>* Configures the maximum burst size, in kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode:** Global configuration
default access-control list *<1-256>* **meter** Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
no access-control list *<1-256>* **meter** Disables the selected ACL meter. **Command mode:** Global configuration
show access-control list *<1-256>* **meter** Displays current ACL Metering parameters. **Command mode:** All

ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL Metering profile, or out of the ACL Metering profile.

Table 201. *ACL Re-Marking Configuration Options*

Command Syntax and Usage
default access-control list *<1-256>* **re-mark** Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
show access-control list *<1-256>* **re-mark** Displays current re-mark parameters. **Command mode:** All

Re-Marking In-Profile Configuration

The following table displays Re-Marking In-Profile configuration commands:

Table 202. *ACL Re-Marking In-Profile Options*

Command Syntax and Usage
access-control list *<1-256>* **re-mark dot1p** *<0-7>* Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
no access-control list *<1-256>* **re-mark dot1p** Disables the use of 802.1p priority for in-profile traffic. **Command mode:** Global configuration
access-control list *<1-256>* **re-mark in-profile dscp** *<0-63>* Re-marks the DSCP value for in-profile traffic. **Command mode:** Global configuration
no access-control list *<1-256>* **re-mark in-profile [dscp]** Deletes the re-mark in-profile configuration. The `dscp` option only disables the use of DSCP for in-profile traffic. **Command mode:** Global configuration
[no] access-control list *<1-256>* **re-mark use-tos-precedence** Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When `enabled`, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration

Re-Marking Out-Profile Configuration

The following table displays Re-Marking Out-Profile configuration commands:

Table 203. *ACL Re-Marking Out-of-Profile Options*

Command Syntax and Usage
access-control list *<1-256>* **re-mark out-profile dscp** *<0-63>* Re-marks the DSCP value on out-of-profile packets for the ACL. **Command mode:** Global configuration
no access-control list *<1-256>* **re-mark out-profile** Disables re-marking on out-of-profile traffic. **Command mode:** Global configuration

ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

Table 204. *IPv6 ACL Options*

Command Syntax and Usage
access-control list6 *<1-128>* **action {permit|deny| |set-priority** *<0-7>***}** Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets or set the 802.1p priority level. **Command mode:** Global configuration
access-control list6 *<1-128>* **action redirect {port** *<port number>***|portchannel** *<1-64>***}** Configures the redirection of packets that match the ACL definitions. You can choose to redirect packets either through an ethernet port or a Link Aggregation Group (LAG). **Command mode**: Global configuration
access-control list6 *<1-128>* **egress-port port** *<port alias or number>* Configures the ACL to function on egress packets. **Command mode:** Global configuration
no access-control list6 *<1-128>* **egress-port port** Disables the ACL to function on egress packets. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **log** Enables or disables Access Control List logging. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **statistics** Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration
default access-control list6 *<1-128>* Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* Displays the current ACL parameters. **Command mode:** All

IPv6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

Table 205. *IP version 6 Filtering Options*

Command Syntax and Usage
access-control list6 *<1-128>* **ipv6 destination-address** *<IPv6 address>* **[***<prefix length (1-128)>***]** Defines a destination IPv6 address for the ACL. If defined, traffic with this destination address will match this ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **ipv6 destination-address** Deletes the configured destination IPv6 address for the specified ACL. **Command mode:** Global configuration
access-control list6 *<1-128>* **ipv6 flow-label** *<0-1048575>* Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **ipv6 flow-label** Deletes the configured flow label for the specified ACL. **Command mode:** Global configuration
access-control list6 *<1-128>* **ipv6 next-header** *<0-255>* Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **ipv6 next-header** Deletes the configured next header for the specified ACL. **Command mode:** Global configuration
access-control list6 *<1-128>* **ipv6 source-address** *<IPv6 address>* **[***<prefix length (1-128)>***]** Defines a source IPv6 address for the ACL. If defined, traffic with this source address will match this ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **ipv6 source-address** Deletes the configured source IPv6 address for the specified ACL. **Command mode:** Global configuration
access-control list6 *<1-128>* **ipv6 traffic-class** *<0-255>* Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL. **Command mode:** Global configuration

Table 205. *IP version 6 Filtering Options*

Command Syntax and Usage
no access-control list6 *<1-128>* **ipv6 traffic-class** Deletes the configured traffic class for the specified ACL. **Command mode:** Global configuration
default access-control list6 *<1-128>* **ipv6** Resets the IPv6 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* **ipv6** Displays the current IPv6 parameters. **Command mode:** All

IPv6 TCP/UDP Filtering Configuration

These commands allows you to define TCP/UDP matching criteria for an ACL.

Table 206. *IPv6 ACL TCP/UDP Filtering Options*

Command Syntax and Usage
access-control list6 *<1-128>* **tcp-udp source-port** *<source port number (1-65535)>* **[***<mask (0xFFFF)>***]** Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports: **Number Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
no access-control list6 *<1-128>* **tcp-udp source-port** Deletes the configured IPv6 source-port for the specified ACL. **Command mode:** Global configuration

Table 206. *IPv6 ACL TCP/UDP Filtering Options*

Command Syntax and Usage
access-control list6 *<1-128>* **tcp-udp destination-port** *<destination port number (1-65535)>* **[***<mask (0xFFFF)>***]** Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `source-port` above. **Command mode:** Global configuration
no access-control list6 *<1-128>* **tcp-udp destination-port** Deletes the configured IPv6 destination-port for the specified ACL. **Command mode:** Global configuration
access-control list6 *<1-128>* **tcp-udp flags** *<value (0x0-0x3f)>* **[***<mask (0x0-0x3f)>***]** Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **tcp-udp flags** Deletes the configured TCP/UDP flag for the specified ACL. **Command mode:** Global configuration
default access-control list6 *<1-128>* **tcp-udp** Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* **tcp-udp** Displays the current TCP/UDP Filtering parameters. **Command mode:** All

IPv6 Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

Table 207. *IPv6 Re-Marking In-Profile Options*

Command Syntax and Usage
default access-control list6 *<1-128>* **re-mark** Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* **re-mark** Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking In-Profile Configuration

The following table displays IPv6 Re-Marking In-Profile configuration commands:

Table 208. *IPv6 ACL Re-Marking In-Profile Options*

Command Syntax and Usage
access-control list6 *<1-128>* **re-mark dot1p** *<0-7>* Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
no access-control6 list6 *<1-128>* **re-mark dot1p** Disables the use of 802.1p priority for in-profile traffic. **Command mode:** Global configuration
access-control list6 *<1-128>* **re-mark in-profile dscp** *<0-63>* Re-marks the DSCP value for in-profile traffic. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark in-profile [dscp]** Deletes the re-mark in-profile configuration. The `dscp` option only disables the use of DSCP for in-profile traffic. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **re-mark use-tos-precedence** Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration

IPv6 Re-Marking Out-Profile Configuration

The following table displays IPv6 Re-Marking Out-Profile configuration commands:

Table 209. *IPv6 ACL Re-Marking Out-of-Profile Options*

Command Syntax and Usage
access-control list6 *<1-128>* **re-mark out-profile dscp** *<0-63>* Re-marks the DSCP value on out-of-profile packets for the ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark out-profile** Disables re-marking on out-of-profile traffic. **Command mode:** Global configuration
show access-control list6 *<1-128>* **re-mark** Displays current re-mark parameters. **Command mode:** All

IPv6 Metering Configuration

These commands define the Access Control profile for the selected ACL.

Table 210. *IPv6 Metering Options*

Command Syntax and Usage
access-control list6 *<1-128>* **meter action {drop|pass}** Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control list6 *<1-128>* **meter committed-rate** *<64-40000000>* Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **meter enable** Enables or disables ACL Metering. **Command mode:** Global configuration
access-control list6 *<1-128>* **meter maximum-burst-size** *<32-4096>* Configures the maximum burst size, in kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode:** Global configuration
default access-control list6 *<1-128>* **meter** Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* **meter** Displays current ACL Metering parameters. **Command mode:** All

ACL Log Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL) log.

Table 211. *ACL Log Configuration Options*

Command Syntax and Usage
[no] access-control list *<1-256>* **log** Enables or disables Access Control List logging. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **log** Enables or disables IPv6 Access Control List logging. **Command mode:** Global configuration
access-control log interval *<5-600>* Sets the filter log displaying interval in seconds. The default setting is `300` seconds. **Command mode:** Global configuration
access-control log rate-limit *<1-1000>* Sets the filter log queue rate limit in packets per second (pps). The default settings is `10` pps. **Command mode:** Global configuration
default access-control log [interval|rate-limit] Resets the specified filter log parameters to their default values. **Command mode:** Global configuration
show access-control log Displays the current ACL log parameters. **Command mode:** All

ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL group. Once you create an ACL group, you can assign the ACL group to one or more ports.

Table 212. *ACL Group Configuration Commands*

Command Syntax and Usage
[no] access-control group *<1-256>* **list** *<1-256>* Adds or removes the selected IPv4 ACL to the ACL group. **Command mode:** Global configuration
[no] access-control group *<1-256>* **list6** *<1-128>* Adds or removes the selected IPv6 ACL to the ACL group. **Command mode:** Global configuration
show access-control group *<1-256>* Displays the current ACL group parameters. **Command mode:** All

Management ACL Configuration

These commands allow you to define filtering criteria for each management ACL (MACL).

Note: Management ACLs (MACLs) are not supported on the management port, only on data ports. Management ACLs filter traffic received through data interfaces only. Management interface is not monitored.

Table 213. *MACL Configuration Options*

Command Syntax and Usage
access-control macl *<1-256>* **action {permit|deny}** Configures a filter action for packets that match the MACL definitions. You can choose to permit (pass) or deny (drop) packets. **Command mode:** Global configuration
[no] access-control macl *<1-256>* **enable** Enables or disables the management ACL. **Command mode:** Global configuration
[no] access-control macl *<1-256>* **statistics** Enables or disables the statistics collection for the MACL. **Command mode:** Global configuration
show access-control macl *<1-256>* Displays the current MACL parameters. **Command mode:** All

MACL IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an MACL.

Table 214. *IP version 4 Filtering Configuration Options*

Command Syntax and Usage
access-control macl *<1-256>* **ipv4 destination-ip-address** *<IP address>* **[***<IP mask>***]** Defines a destination IP address for the MACL. If defined, traffic with this destination IP address will match this MACL. **Command mode:** Global configuration
no access-control macl *<1-256>* **ipv4 destination-ip-address** Deletes the configured destination IP address for the specified MACL. **Command mode:** Global configuration

Table 214. *IP version 4 Filtering Configuration Options*

Command Syntax and Usage
access-control macl *<1-256>* **ipv4 protocol** *<0-255>* Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number** **Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp **Command mode:** Global configuration
no access-control macl *<1-256>* **ipv4 protocol** Deletes the configured IP protocol for the specified MACL. **Command mode:** Global configuration
access-control macl *<1-256>* **ipv4 source-ip-address** *<IP address>* **[***<IP mask>***]** Defines a source IP address for the MACL. If defined, traffic with this source IP address will match this MACL. Specify an IP address in dotted decimal notation. **Command mode:** Global configuration
no access-control macl *<1-256>* **ipv4 source-ip-address** Deletes the configured source IP address for the specified MACL. **Command mode:** Global configuration
no access-control macl *<1-256>* **ipv4** Removes all the IPv4 parameters for the specified MACL. **Command mode:** Global configuration
show access-control macl *<1-256>* **ipv4** Displays the current IPv4 parameters. **Command mode:** All

MACL TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an MACL.

Table 215. *TCP/UDP Filtering Configuration Options*

Command Syntax and Usage
access-control macl *<1-256>* **tcp-udp source-port** *<1-65535>* **[**<*mask (0xFFFF)*>**]** Defines a source port for the MACL. If defined, traffic with the specified TCP or UDP source port will match this MACL. Specify the port number. Listed below are some of the well-known ports: **Number** **Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
no access-control macl *<1-256>* **tcp-udp source-port** Deletes the configured source port for the specified MACL. **Command mode:** Global configuration
access-control macl *<1-256>* **tcp-udp destination-port** *<1-65535>* **[**<*mask (0xFFFF)*>**]** Defines a destination port for the MACL. If defined, traffic with the specified TCP or UDP destination port will match this MACL. Specify the port number, just as with `source-port` above. **Command mode:** Global configuration
no access-control macl *<1-256>* **tcp-udp destination-port** Deletes the configured destination port for the specified MACL. **Command mode:** Global configuration
default access-control macl *<1-256>* **tcp-udp** Resets the TCP/UDP parameters for the MACL to their default values. **Command mode:** Global configuration
show access-control macl *<1-256>* **tcp-udp** Displays the current TCP/UDP Filtering parameters. **Command mode:** All

VMAP Configuration

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see "Access Control List Configuration" on page 426.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration" on page 501.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 642.

The following table lists the general VMAP configuration commands.

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
access-control vmap *<1-128>* **action {permit|deny|set-priority** *<0-7>***}** Configures a filter action for packets that match the VMAP definitions. You can choose to permit (pass) or deny (drop) packets or set the 802.1p priority level. **Command mode:** Global configuration
access-control vmap *<1-128>* **action redirect {port** *<port alias or number>***|portchannel** *<1-144>***}** Configures the switch to redirect traffic that matches the VMAP definitions to a specific port or Link Aggregation Group (LAG). **Command mode**: Global configuration
access-control vmap *<1-128>* **egress-port** *<port alias or number>* Configures the VMAP to function on egress packets. **Command mode:** Global configuration
no access-control vmap *<1-128>* **egress-port** Disables the VMAP to function on egress packets. **Command mode:** Global configuration
access-control vmap *<1-128>* **ethernet destination-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the destination MAC address for the VMAP. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet destination-mac-address** Removes the destination MAC address for the specified VMAP. **Command mode:** Global configuration

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
access-control vmap *<1-128>* **ethernet ethernet-type {***<0x600-0xFFFF>***|any|arp|ip|ipv6|mpls|rarp}** Defines the Ethernet type for the VMAP. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet ethernet-type** Removes the Ethernet type for the specified VMAP. **Command mode:** Global configuration
access-control vmap *<1-128>* **ethernet priority** *<0-7>* Defines the Ethernet priority value for the VMAP. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet priority** Removes the Ethernet priority for the specified VMAP. **Command mode:** Global configuration
access-control vmap *<1-128>* **ethernet source-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the source MAC address for the VMAP. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet source-mac-address** Removes the source MAC address for the specified VMAP. **Command mode:** Global configuration
access-control vmap *<1-128>* **ethernet vlan** *<VLAN ID (1-4094)>* **[***<VLAN mask>***]** Defines a VLAN number and mask for the VMAP. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet vlan** Removes the VLAN number and mask for the specified VMAP. **Command mode:** Global configuration
default access-control vmap *<1-128>* **ethernet** Resets Ethernet parameters for the VMAP to their default values. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ethernet** Resets Ethernet header parameters for the VMAP to their default values. **Command mode:** Global configuration

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
access-control vmap *<1-128>* **ipv4 destination-ip-address** *<IPv4 address>* **[***<IPv4 mask>***]** Enables filtering of VMAP statistics collection based on destination IP address. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ipv4 destination-ip-address** Disables filtering of VMAP statistics collection based on destiantion IP address. **Command mode:** Global configuration
access-control vmap *<1-128>* **ipv4 protocol** *<0-255>* Enables filtering of VMAP statistics collection based on protocol. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ipv4 protocol** Disables filtering of VMAP statistics collection based on protocol. **Command mode:** Global configuration
access-control vmap *<1-128>* **ipv4 source-ip-address** *<IPv4 address>* **[***<IPv4 mask>***]** Enables filtering of VMAP statistics collection based on source IP address. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ipv4 source-ip-address** Disables filtering of VMAP statistics collection based on source IP address. **Command mode:** Global configuration
access-control vmap *<1-128>* **ipv4 type-of-service** *<0-255>* Enables filtering of VMAP statistics collection based on type of service. **Command mode:** Global configuration
no access-control vmap *<1-128>* **ipv4 type-of-service** Disables filtering of VMAP statistics collection based on type of service. **Command mode:** Global configuration
default access-control vmap *<1-128>* **ipv4** Resets the IPv4 parameters for the VMAP to their default values. **Command mode:** Global configuration
access-control vmap *<1-128>* **meter action {drop|pass}** Sets VMAP port metering to drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control vmap *<1-128>* **meter committed-rate** *<64-40000000>* Sets the VMAP port metering control rate in kilobits per second. **Command mode:** Global configuration

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
`[no] access-control vmap` *<1-128>* **`meter enable`** Enables or disables VMAP port metering. **Command mode:** Global configuration
`access-control vmap` *<1-128>* **`meter maximum-burst-size`** *<32-4096>* Sets the VMAP port metering maximum burst size in kilobits. The following eight values are allowed: `32`, `64`, `128`, `256`, `512`, `1024`, `2048` or `4096`. **Command mode:** Global configuration
`default access-control vmap` *<1-128>* **`meter`** Resets the VMAP meter configuration to its default values. **Command mode:** Global configuration
`access-control vmap` *<1-128>* **`mirror port`** *<port alias or number>* Sets the specified port as the mirror target. **Command mode:** Global configuration
`no access-control vmap` *<1-128>* **`mirror`** Disables VMAP mirroring. **Command mode:** Global configuration
`access-control vmap` *<1-128>* **`packet-format ethernet {ethernet-type2|llc|snap}`** Sets to filter the specified ethernet packet format type. **Command mode:** Global configuration
`access-control vmap` *<1-128>* **`packet-format ip {ipv4|ipv6}`** Sets to filter the specified IP packet format type. **Command mode:** Global configuration
`access-control vmap` *<1-128>* **`packet-format tagging {any|none| |tagged}`** Sets to filter the based on packet tagging. The options are: o `any`: Filter tagged & untagged packets o `none`: Filter only untagged packets o `tagged`: Filter only tagged packets **Command mode:** Global configuration
`no access-control vmap` *<1-128>* **`packet-format {ethernet|ip| |tagging}`** Disables filtering based on the specified packet format. **Command mode:** Global configuration

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
default access-control vmap *<1-128>* **packet-format** Resets the VMAP packet-format configuration to its default values. **Command mode:** Global configuration
access-control vmap *<1-128>* **re-mark dot1p** *<0-7>* Sets the VMAP re-mark configuration user update priority. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark dot1p** Disables the use of dot1p for in-profile traffic VMAP re-mark configuration. **Command mode:** Global configuration
access-control vmap *<1-128>* **re-mark {in-profile|out-profile} dscp** *<0-63>* Sets the VMAP re-mark configuration user update priority for in-profile or out-profile traffic. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark {in-profile| |out-profile}** Removes all re-mark in-profile or out-profile settings. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark in-profile dscp** Disables the use of DSCP for in-profile traffic. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **re-mark use-tos-precedence** Enables or disables the use of the TOS precedence for in-profile traffic. **Command mode:** Global configuration
default access-control vmap *<1-128>* **re-mark** Resets the VMAP re-mark parameters to their default values. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark** Disables re-marking for the specified VMAP. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **statistics** Enables or disables statistics for this access control list. **Command mode:** Global configuration

Table 216. *VMAP Configuration Options*

Command Syntax and Usage
access-control vmap *<1-128>* **tcp-udp {source-port| |destination-port}** *<1-65535>* **[***<port mask (0x0001 - 0xFFFF)>***]** Sets the TCP/UDP filtering source port or destination port and port mask for this ACL. **Command mode:** Global configuration
access-control vmap *<1-128>* **tcp-udp flags** *<0x0-0x3F>* **[***<flags mask (0x0-0x3F)>***]** Sets the TCP flags for this ACL. **Command mode:** Global configuration
default access-control vmap *<1-128>* **tcp-udp** Resets the TCP/UDP parameters for the VMAP to their default values. **Command mode:** Global configuration
no access-control vmap *<1-128>* **tcp-udp** Removes TCP/UDP filtering for this ACL. **Command mode:** Global configuration
default access-control vmap *<1-128>* Resets the VMAP parameters to their default values. **Command mode:** Global configuration
no access-control vmap *<1-128>* Deletes the specified VMAP. **Command mode:** Global configuration
show access-control vmap [*<1-128>***]** Displays the current VMAP parameters. **Command mode:** All

Port Mirroring

Port Mirroring is disabled by default. For more information about port mirroring on the G8272, see "Appendix A: Troubleshooting" in the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Port Mirroring commands are used to configure, enable and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 217. *Port Mirroring Configuration Options*

Command Syntax and Usage
[no] port-mirroring enable Enables or disables port mirroring. **Command mode:** Global configuration
show port-mirroring Displays current settings of the mirrored and monitoring ports. **Command mode:** All

Port-Mirroring Configuration

The following table describes the Port Mirroring commands.

Table 218. *Port-Based Port-Mirroring Configuration Options*

Command Syntax and Usage
port-mirroring monitor-port *<port alias or number>* **mirroring-port** *<port alias or number>* **{in|out|both}** Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port. If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port. **Command mode:** Global configuration
no port-mirroring monitor-port *<port alias or number>* **[mirroring-port** *<port alias or number>***]** Removes the monitor port. The `mirroring-port` option only removes the mirrored port. **Command mode:** Global configuration
show port-mirroring Displays the current settings of the monitoring port. **Command mode:** All

Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 219. *Layer 2 Configuration Commands*

Command Syntax and Usage
vlan *<VLAN ID (1-4094)>* Enter VLAN configuration mode. If the specified VLAN(s) doesn't exist, it will be created. To view command options, see page 501. **Command mode:** Global configuration
show layer2 Displays current Layer 2 parameters. **Command mode:** All

802.1X Configuration

These commands allow you to configure the G8272 as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 220. *802.1x Configuration Options*

Command Syntax and Usage
[no] dot1x enable Globally enables or disables 802.1X. **Command mode:** Global configuration
show dot1x Displays current 802.1X parameters. **Command mode:** All

The following sections describe the 802.1x configuration options:

- "802.1X Global Configuration" on page 456
- "802.1X Guest VLAN Configuration" on page 458
- "802.1X Port Configuration" on page 459

802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the switch.

Table 221. *802.1X Global Configuration Options*

Command Syntax and Usage
dot1x max-request *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. **Command mode:** Global configuration
dot1x mode {force-unauthorized|auto|force-authorized} Sets the type of access control for all ports: o force-unauthorized - the port is unauthorized unconditionally. o auto - the port is unauthorized until it is successfully authorized by the RADIUS server. o force-authorized - the port is authorized unconditionally, allowing all traffic. The default value is force-authorized. **Command mode:** Global configuration
dot1x quiet-time *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Global configuration
[no] dot1x re-authenticate Sets the re-authentication status to on or off. The default value is off. **Command mode:** Global configuration
dot1x re-authentication-interval *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Global configuration

Table 221. *802.1X Global Configuration Options (continued)*

Command Syntax and Usage
dot1x server-timeout *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is `30` seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of **radius-server timeout** *<1-10>* (default is `3` seconds). **Command mode:** Global configuration
dot1x supplicant-timeout *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is `30` seconds. **Command mode:** Global configuration
dot1x transmit-interval *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is `30` seconds. **Command mode:** Global configuration
[no] dot1x vlan-assign Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. **Command mode:** Global configuration
default dot1x Resets the global 802.1X parameters to their default values. **Command mode:** Global configuration
show dot1x Displays current global 802.1X parameters. **Command mode:** All

802.1X Guest VLAN Configuration

The 802.1X Guest VLAN commands allow you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 222. *802.1X Guest VLAN Configuration Options*

Command Syntax and Usage
[no] dot1x guest-vlan enable Enables or disables the 802.1X Guest VLAN. **Command mode:** Global configuration
dot1x guest-vlan vlan *<VLAN ID (1-4094)>* Configures the Guest VLAN number. **Command mode:** Global configuration
no dot1x guest-vlan vlan Removes the Guest VLAN number. **Command mode:** Global configuration
show dot1x Displays current 802.1X parameters. **Command mode:** All

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the switch. These settings override the global 802.1X parameters.

Table 223. *802.1X Port Options*

Command Syntax and Usage
dot1x apply-global Applies current global 802.1X configuration parameters to the port. **Command mode:** Interface port
dot1x max-request *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. **Command mode:** Interface port
dot1x mode {auto|force-authorized|force-unauthorized} Sets the type of access control for the port: o auto - the port is unauthorized until it is successfully authorized by the RADIUS server. o force-authorized - the port is authorized unconditionally, allowing all traffic. o force-unauthorized - the port is unauthorized unconditionally. The default value is force-authorized. **Command mode:** Interface port
dot1x quiet-time *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Interface port
[no] dot1x re-authenticate Sets the re-authentication status to on or off. The default value is off. **Command mode:** Interface port
dot1x re-authentication-interval *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Interface port

Table 223. *802.1X Port Options (continued)*

Command Syntax and Usage
dot1x server-timeout *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is `30` seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the **radius-server timeout** *<1-10>* command. **Command mode:** Interface port
dot1x supplicant-timeout *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is `30` seconds. **Command mode:** Interface port
dot1x transmit-interval *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is `30` seconds. **Command mode:** Interface port
[no] dot1x vlan-assign Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. **Command mode:** Interface port
default dot1x Resets the 802.1X port parameters to their default values. **Command mode:** Interface port
show interface port *<port alias or number>* **dot1x** Displays current 802.1X port parameters. **Command mode:** All

Spanning Tree Configuration

Enterprise NOS supports the IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). The Spanning Tree Protocol (STP) is used to prevent loops in the network topology.

Up to 256 Spanning Tree Groups can be configured on the switch (STG 256 is reserved for management). By default, 128 STGs are configured (STG 128 is reserved for management).

Note: When VRRP is used for active/active redundancy, STG must be enabled.

Table 224. *Spanning Tree Configuration Options*

Command Syntax and Usage
`spanning-tree loopguard` Enables STP loop guard. STP loop guard prevents ports from forwarding traffic if no BPDUs are received. Ports are placed into a loop-inconsistent blocking state until a BPDU is received. **Command mode:** Global configuration
`spanning-tree mode [disable|mst|pvrst|rstp]` Selects and enables Multiple Spanning Tree mode (`mst`), Per VLAN Rapid Spanning Tree mode (`pvrst`) or Rapid Spanning Tree mode (`rstp`). The default mode is `PVRST`. When you select the `disable` option, the switch globally turns Spanning Tree `off`. All ports are placed into forwarding state. Any BPDU's received are flooded. **Command mode:** Global configuration
`[no] spanning-tree pvst-compatibility` Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is `enabled`. **Command mode:** Global configuration
`[no] spanning-tree stg-auto` Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool. **Notes**: o When using VASA, a maximum number of 255 automatically assigned STGs is supported. o VASA applies only to PVRST mode. **Command mode:** Global configuration

Table 224. *Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
spanning-tree guard loop Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received. **Command mode:** Interface port/Interface portchannel
spanning-tree guard root Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening). **Command mode:** Interface port/Interface portchannel
spanning-tree guard none Disables STP loop guard and root guard. **Command mode:** Interface port/Interface portchannel
no spanning-tree guard Sets the Spanning Tree guard parameters to their default values. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree link-type {p2p|shared|auto} Defines the type of link connected to the port, as follows: o `auto`: Configures the port to detect the link type, and automatically match its settings. o `p2p`: Configures the port for Point-To-Point protocol. o `shared`: Configures the port to connect to a shared medium (usually a hub). The default link type is `auto`. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree portfast Enables or disables this port as portfast or edge port. An edge port is not connected to a bridge and can begin forwarding traffic as soon as the link is up. Configures server ports as edge ports (`enabled`). **Note**: After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree pvst-protection Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST BPDUs it becomes error disabled. PVST Protection works only in MSTP mode. The default setting is `disabled`. **Command mode:** Interface port/Interface portchannel

Table 224. *Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
show spanning-tree Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST or MSTP) and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: o Priority o Hello interval o Maximum age value o Forwarding delay o Aging time You can also see the following port-specific STG information: o Port alias and priority o Cost o State **Command mode:** All
show spanning-tree root Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see page 77. **Command mode:** All
show spanning-tree blockedports Lists the ports blocked by each STP instance. **Command mode:** All
show spanning-tree [vlan *<VLAN ID (1-4094)>***] bridge** Displays Spanning Tree bridge information. For details, see page 76. **Command mode:** All

MSTP Configuration

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MSTP is turned off by default and the default STP mode is PVRST.

Note: When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

Table 225. *Multiple Spanning Tree Configuration Options*

Command Syntax and Usage
spanning-tree mst configuration Enables MSTP configuration mode. **Command mode:** Global configuration
[no] spanning-tree mst *<0-32>* **enable** Enables or disables the specified MSTP instance. **Command mode:** Global configuration
spanning-tree mst *<0-32>* **priority** *<0-65535>* Configures the bridge priority for the specified MSTP instance. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192, 12288 ...) and the default value is `32768`. **Command mode:** Global configuration
no spanning-tree mst *<0-32>* **priority** Resets the bridge priority for the specified MSTP instance to the default value of `32768`. **Command mode:** Global configuration
spanning-tree mst forward-time *<4-30>* Configures the forward delay time in seconds. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the discarding and learning states to the forwarding state. The default value is `15`. **Command mode:** Global configuration
spanning-tree mst max-age *<6-40>* Configures the maximum age interval in seconds. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The default value is `20` seconds. **Command mode:** Global configuration

Table 225. *Multiple Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
spanning-tree mst max-hops *<4-60>* Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is 20 hops. **Command mode:** Global configuration
instance *<0-32>* **vlan** *<VLAN ID (1-4094)>* Map the specified VLANs to the Spanning Tree instance. If a VLAN does not exist, it is not created automatically. **Note**: This command becomes visible only when the spanning tree mode is MSTP. **Command mode:** MST configuration
no instance *<0-32>* **vlan {***<VLAN ID (1-4094)>***|all}** Remove the specified VLANs or all VLANs from the Spanning Tree instance. **Command mode:** MST configuration
name *<1-32 characters>* Configures a name for the MSTP region. All devices within an MSTP region must have the same region name. **Command mode:** MST configuration
no name Clears the name of the MSTP region. **Command mode:** MST configuration
revision *<0-65535>* Configures a revision number for the MSTP region. The revision is used as a numerical identifier for the region. All devices within an MSTP region must have the same revision number. **Command mode:** MST configuration
no revision Resets the revision number for the MSTP region. **Command mode:** MST configuration
default spanning-tree mst *<0-32>* Restores a Spanning Tree instance or range of instances to default configuration. **Command mode:** Global configuration

Table 225. *Multiple Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
show spanning-tree mst configuration Displays the current MSTP settings. **Command mode:** All
show spanning-tree mst *<0-32>* **information** Displays current MST information for the specified instance. **Command mode:** All

MSTP Port Configuration

MSTP port parameters are used to modify MSTP operation on an individual port basis. MSTP parameters do not affect operation of RSTP/PVRST. For each port, RSTP/PVRST/MSTP is turned on by default.

Table 226. *MSTP Port Configuration Options*

Command Syntax and Usage
spanning-tree mst *<0-32>* **cost** *<0-200000000>* Configures the port path cost for the specified MSTP instance. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: o 1Gbps = 20000 o 10Gbps = 2000 The default value of `0` (zero) indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree mst *<0-32>* **enable** Enables or disables the specified MSTP instance on the port. **Command mode:** Interface port/Interface portchannel
spanning-tree mst *<0-32>* **port-priority** *<0-240>* Configures the port priority for the specified MSTP instance. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is `128`. **Command mode:** Interface port/Interface portchannel

Table 226. *MSTP Port Configuration Options (continued)*

Command Syntax and Usage
spanning-tree mst hello-time *<1-10>* Configures the port Hello time.The Hello time specifies how often the bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds and the default is 2 seconds. **Command mode:** Interface port/Interface portchannel
show interface port *<port alias or number>* **spanning-tree mstp cist** Displays the current CIST port configuration. **Command mode:** All

RSTP/PVRST Configuration

The following table describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST) protocols.

Table 227. *RSTP/PVRST Configuration Options*

Command Syntax and Usage
boot spanning-tree max-instances {128|256} Configures the maximum number of Spanning Tree Groups (STGs) that can be used on the switch. The default value is 128. **Note**: The switch needs to be reloaded for the configuration to take effect. **Command mode**: Global configuration
no boot spanning-tree max-instances Reset the maximum number of STGs available on the switch to the default value of 128. **Note**: The switch needs to be reloaded for the configuration to take effect. **Command mode**: Global configuration
[no] spanning-tree stp *<1-256>* **enable** Globally enables or disables Spanning Tree Protocol. STG is turned on by default. **Command mode:** Global configuration
spanning-tree stp *<1-256>* **vlan** *<VLAN ID (1-4094)>* Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will not be enabled by default. **Command mode:** Global configuration
no spanning-tree stp *<1-256>* **vlan {***<VLAN ID (1-4094)>***|all}** Breaks the association between a specified VLAN or all VLANs and a Spanning Tree Group and requires a VLAN ID as a parameter. **Command mode:** Global configuration
default spanning-tree stp *<1-256>* Restores a Spanning Tree instance to its default configuration. **Command mode:** Global configuration

Table 227. *RSTP/PVRST Configuration Options (continued)*

Command Syntax and Usage
`show boot spanning-tree` Displays the maximum number of currently available STGs on the switch and the maximum number of available STGs after the switch reloads. For a sample output, see page 702. **Command mode**: All
`show spanning-tree stp` *<1-256>* Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See page 71 for details about the `information` parameter. **Command mode:** All

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

When configuring STG bridge parameters, the following formulas must be used:

- 2 × (*forwarding delay* - 1) ≥ *bridge maximum age*
- 2 × (*bridge hello time* + 1) ≤ *bridge maximum age*

Table 228. *Bridge Spanning Tree Configuration Options*

Command Syntax and Usage
spanning-tree stp *<1-256>* **bridge forward-delay** *<4-30>* Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the discarding and learning states to the forwarding state. The range is 4 to 30 seconds and the default is `15` seconds. **Note:** This command does not apply to MSTP. **Command mode:** Global configuration
no spanning-tree stp *<1-256>* **bridge forward-delay** Resets the bridge forward delay parameter to its default value of `15` seconds. **Command mode:** Global configuration
spanning-tree stp *<1-256>* **bridge hello-time** *<1-10>* Configures the bridge Hello time.The Hello time specifies how often the bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds and the default is `2` seconds. **Note:** This command does not apply to MSTP. **Command mode:** Global configuration
no spanning-tree stp *<1-256>* **bridge hello-time** Resets the birdge Hello time to its default value of `2` seconds. **Command mode:** Global configuration
spanning-tree stp *<1-256>* **bridge maximum-age** *<6-40>* Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds and the default is `20` seconds. **Note:** This command does not apply to MSTP. **Command mode:** Global configuration

Table 228. *Bridge Spanning Tree Configuration Options*

Command Syntax and Usage
no spanning-tree stp *<1-256>* **bridge maximum-age** Resets the bridge maximum age to its default value of `20` seconds. **Command mode:** Global configuration
spanning-tree stp *<1-256>* **bridge priority** *<0-65535>* Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. Enter the value in multiples of 4096. Non-multiples are automatically rounded up to the closest valid priority. The default value is `32768`. **Command mode:** Global configuration
no spanning-tree stp *<1-256>* **bridge priority** Resets the bridge priority to its default value of `32768`. **Command mode:** Global configuration
show spanning-tree [vlan *<VLAN ID (1-4094)>***] bridge** Displays the current Spanning Tree parameters either globally or for a specific VLAN. See page 76 for sample output. **Command mode:** All

By default, Spanning Tree is turned `off` for management ports, and turned `on` for data ports. STG port parameters include:

- Port priority
- Port path cost

Table 229. *Spanning Tree Port Options*

Command Syntax and Usage
`[no] spanning-tree stp` *<1-256>* **`enable`** Enables or disables STG on the port. **Command mode:** Interface port/Interface portchannel
`spanning-tree stp` *<1-256>* **`path-cost`** *<1-200000000, 0 for default)>* Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: o 1Gbps = 20000 o 10Gbps = 2000 The default value of `0` (zero) indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port/Interface portchannel
`spanning-tree stp` *<1-256>* **`priority`** *<0-240>* Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is `128`. **RSTP/PVRST**: The range is 0 to 240, in steps of 16 (0, 16, 32...). **Command mode:** Interface port/Interface portchannel
`default spanning-tree stp` *<1-256>* Resets the STG configuration to its default settings. **Command mode:** Interface port/Interface portchannel
`show interface port` *<port alias or number>* **`spanning-tree stp`** *<1-256>* Displays the current STG port parameters. **Command mode:** All

Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 230. *FDB Configuration Options*

Command Syntax and Usage
mac-address-table aging *<0-65535>* Configures the aging value for FDB entries, in seconds. The default value is `300` seconds. **Command mode**: Global configuration
mac-address-table multicast Configures multicast FDB entries. For command options, see page 474. **Command mode:** Global configuration
mac-address-table static Configures static FDB entries. For command options, see page 475. **Command mode:** Global configuration
show mac-address-table Display current FDB configuration. **Command mode**: All

Static Multicast MAC Configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**`mac-address-table multicast`**).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
  - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (**`mac-address-table multicast`**).
  - Enable Flood Blocking on ports that are not to receive multicast packets (**`interface port`** *<port alias or number>*) (**`flood-blocking`**).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

Table 231. *Static Multicast MAC Configuration Options*

Command Syntax and Usage
`[no] mac-address-table multicast` *<MAC address> <VLAN ID (1-4094)> <port alias or number>* Adds or removes a static multicast entry. You can list ports separated by a comma (`,`) or enter a range of ports separated by a hyphen (`-`). For example: **`mac-address-table multicast`** `01:00:00:23:3f:01 200 1-4` **Command mode**: Global configuration
`[no] mac-address-table multicast` *<MAC address>* **`port`** *<port alias or number>* Adds or removes a static multicast entry for Network Load Balancing (NLB). You can list ports separated by a comma (`,`) or enter a range of ports separated by a hyphen (`-`). For example: **`mac-address-table multicast`** `01:00:00:23:3f:01` **`port`** `1-4` **Command mode**: Global configuration
`mac-address-table multicast reload` Reloads all static multicast entries. **Command mode:** Global configuration

Table 231. *Static Multicast MAC Configuration Options*

Command Syntax and Usage
no mac-address-table multicast all [interface port *<port number or alias>***|mac** *<MAC address>***|vlan** *<VLAN ID (1-4094)>***]** Deletes all static multicast entries. o `interface port` deletes all static multicast entries that use the specified port o `mac` deletes all static multicast entries that use the specified MAC address o `vlan` deletes all static multicast entries that use the specified vlan **Command mode**: Global configuration
show mac-address-table multicast Display the current static multicast entries. **Command mode**: All

Static FDB Configuration

Use the following commands to configure static entries in the Forwarding Database (FDB).

Table 232. *FDB Configuration Options*

Command Syntax and Usage
[no] mac-address-table static *<MAC address>* **port** *<port alias or number>* Adds or removes a permanent FDB entry. Enter the MAC address using the following format: `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address as follows: `xxxxxxxxxxxx`. For example, `080020123456`. **Command mode:** Global configuration
mac-address-table static *<MAC address>* **vlan** *<VLAN ID (1-4094)>* **{port** *<port alias or number>***|portchannel** *<1-72>***|adminkey** *<1-65535>***}** Adds a permanent FDB entry. Enter the MAC address using the following format: `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address as follows: `xxxxxxxxxxxx`. For example, `080020123456`. **Command mode**: Global configuration
no mac-address-table static *<MAC address> <VLAN ID (1-4094)>* Deletes permanent FDB entries. **Command mode**: Global configuration

Table 232. *FDB Configuration Options*

Command Syntax and Usage
no mac-address-table static all [mac *<MAC address>***| vlan** *<VLAN ID (1-4094)>***]** Deletes all permanent FBD entries. o `mac` deletes all permanent entries that use the specified MAC address o `vlan` deletes all permanent entries that use the specified vlan **Command mode**: Global configuration
no mac-address-table static all interface {port *<port alias or number>***|portchannel** *<1-72>***|adminkey** *<1-65535>***}** Deletes all permanent FBD entries that use the specified port, Link Aggregation Group (LAG) or LACP admin key. **Command mode:** Global configuration
show mac-address-table Display current FDB configuration. **Command mode**: All

ECP Configuration

Use the following commands to configure Edge Control Protocol (ECP).

Table 233. *ECP Configuration Options*

Command Syntax and Usage
ecp retransmit-interval *<100-9000>* Configures ECP retransmit interval in milliseconds. The default value is `1000` miliseconds. **Command mode**: Global configuration
default ecp retransmit-interval Resets the ECP retransmit interval to the default `1000` milliseconds. **Command mode**: Global configuration
show ecp [channels|retransmit-interval| upper-layer-protocols] Displays settings for the ECP retransmit interval or for all ECP channels or registered ULPs. **Command mode**: All

LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 234. *LLDP Configuration Options*

Command Syntax and Usage
`[no] lldp enable` Globally enables or disables LLDP. The default setting is `enabled`. **Command mode**: Global configuration
`lldp holdtime-multiplier` *<2-10>* Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is `4`. **Command mode**: Global configuration
`no lldp holdtime-multiplier` Resets the message hold time multiplier to its default value of `4`. **Command mode:** Global configuration
`lldp refresh-interval` *<5-32768>* Configures the message transmission interval, in seconds. The default value is `30` seconds. **Command mode**: Global configuration
`no lldp refresh-interval` Resets the message transmission interval to its default value of `30` seconds. **Command mode:** Global configuration
`lldp reinit-delay` *<1-10>* Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages. The default value is `2` seconds. **Command mode**: Global configuration
`no lldp reinit-delay` Resets the re-initialization delay interval to its default value of *2* seconds. **Command mode:** Global configuration
`lldp transmission-delay` *<1-8192>* Configures the transmission delay interval, in seconds. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port. The default value is `2` seconds. **Command mode**: Global configuration

Table 234. *LLDP Configuration Options (continued)*

Command Syntax and Usage
no lldp transmission-delay Resets the transmission delay interval to its default value of 2 seconds. **Command mode:** Global configuration
lldp trap-notification-interval *<1-3600>* Configures the trap notification interval, in seconds. The default value is 5 seconds. **Command mode**: Global configuration
no lldp trap-notification-interval Resets the trap notification interval to its default value of 5 seconds. **Command mode:** Global configuration
show lldp [port [*<port alias or number>***]]** Display current LLDP configuration. **Command mode**: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 235. *LLDP Port Options*

Command Syntax and Usage
lldp admin-status {tx_only|rx_only|tx_rx} Configures the LLDP transmission type for the port, as follows: o Transmit only o Receive only o Transmit and receive The default setting is tx_rx. **Command mode**: Interface port
no lldp admin-status Disables the LLDP transmission type. **Command mode**: Interface port
[no] lldp trap-notification Enables or disables SNMP trap notification for LLDP messages. **Command mode**: Interface port
show interface port *<port alias or number>* **lldp** Display current LLDP port configuration. **Command mode**: All

LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 236. *Optional TLV Options*

Command Syntax and Usage
[no] lldp tlv all Enables or disables all optional TLV information types. **Command mode**: Interface port
[no] lldp tlv dcbx Enables or disables the DCBX information type. **Command mode**: Interface port
[no] lldp tlv framesz Enables or disables the Maximum Frame Size information type. **Command mode**: Interface port
[no] lldp tlv linkaggr Enables or disables the Link Aggregation information type. **Command mode**: Interface port
[no] lldp tlv macphy Enables or disables the MAC/Phy Configuration information type. **Command mode**: Interface port
[no] lldp tlv mgmtaddr Enables or disables the Management Address information type. **Command mode**: Interface port
[no] lldp tlv portdesc Enables or disables the Port Description information type. **Command mode**: Interface port
[no] lldp tlv portprot Enables or disables the Port and VLAN Protocol ID information type. **Command mode**: Interface port
[no] lldp tlv portvid Enables or disables the Port VLAN ID information type. **Command mode**: Interface port

Table 236. *Optional TLV Options (continued)*

Command Syntax and Usage
[no] lldp tlv powermdi Enables or disables the Power via MDI information type. **Command mode**: Interface port
[no] lldp tlv protid Enables or disables the Protocol ID information type. **Command mode**: Interface port
[no] lldp tlv syscap Enables or disables the System Capabilities information type. **Command mode**: Interface port
[no] lldp tlv sysdescr Enables or disables the System Description information type. **Command mode**: Interface port
[no] lldp tlv sysname Enables or disables the System Name information type. **Command mode**: Interface port
[no] lldp tlv vlanname Enables or disables the VLAN Name information type. **Command mode**: Interface port
show interface port *<port alias or number>* **lldp** Display current LLDP port configuration. **Command mode**: All

Link Aggregation Group (LAG) Configuration

Link Aggregation Groups (LAGs) can provide super-bandwidth connections between RackSwitch G8272s or other aggregation capable devices. A *LAG* is a group of ports that act together, combining their bandwidth to create a single, larger port. Two types of aggregation are available: static LAGs (portchannels) and dynamic LACP LAGs (portchannels).

The two types of aggregation can be configured using the following portchannel ranges:

- static LAGs: 1-72
- LACP LAGs: 73-144

Up to 72 static LAGs can be configured on the G8272, with the following restrictions:

- Any physical switch port can belong to no more than one LAG.
- Up to 32 ports can belong to the same LAG.
- You must configure all ports in a LAG with the same properties (speed, duplex, flow control, STG, VLAN and so on).
- Aggregation from non-Lenovo devices must comply with Cisco® EtherChannel® technology.

By default, each LAG is empty and disabled.

Table 237. *LAG Configuration Options*

Command Syntax and Usage
[no] portchannel *<1-72>* **enable** Enables or disables the current LAG. **Command mode:** Global configuration
portchannel *<1-72>* **port** *<port alias or number>* **[enable]** Adds a physical port or ports to the current LAG. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-). The `enable` option also enables the current LAG. **Command mode:** Global configuration
no portchannel *<1-72>* **port** *<port alias or number>* Removes a physical port or ports from the current LAG. **Command mode:** Global configuration
no portchannel *<1-72>* Removes the current LAG configuration. **Command mode:** Global configuration
show portchannel *<1-72>* Displays current LAG parameters. **Command mode:** All

Link Aggregation Group (LAG) Hash Configuration

Use the following commands to configure Link Aggregation Group (LAG) hash settings for the G8272. The LAG hash settings affect both static LAGs and LACP LAGs.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in Table 238 combined with the hash parameters listed in Table 239 and Table 240.

Table 238. *LAG Hash Options*

Command Syntax and Usage
`[no] portchannel thash fcoe cntag-id` Enables or disables FCoE LAG hashing on the cntag id. **Command mode:** Global configuration
`[no] portchannel thash fcoe destination-id` Enables or disables FCoE LAG hashing on the destination id. **Command mode:** Global configuration
`[no] portchannel thash fcoe fabric-id` Enables or disables FCoE LAG hashing on the fabric id. **Command mode:** Global configuration
`[no] portchannel thash fcoe originator-id` Enables or disables FCoE LAG hashing on the originator id. **Command mode:** Global configuration
`[no] portchannel thash fcoe responder-id` Enables or disables FCoE LAG hashing on the responder id. **Command mode:** Global configuration
`[no] portchannel thash fcoe source-id` Enables or disables FCoE LAG hashing on the source id. **Command mode:** Global configuration
`[no] portchannel thash ingress` Enables or disables LAG hash computation based on the ingress port. The default setting is `disabled`. **Command mode:** Global configuration

Table 238. *LAG Hash Options*

Command Syntax and Usage
`[no] portchannel thash L4port` Enables or disables use of Layer 4 service ports (TCP, UDP and so on) to compute the hash value. The default setting is `disabled`. **Command mode:** Global configuration
`show portchannel hash` Display current LAG hash configuration. **Command mode**: All

Layer 2 Link Aggregation Group (LAG) Hash

Layer 2 Link Aggregation Group (LAG) hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 LAG hash parameters for the switch.

Table 239. *Layer 2 LAG Hash Options*

Command Syntax and Usage
portchannel thash l2thash l2-destination-mac-address Enables Layer 2 LAG hashing on the destination MAC. **Command mode:** Global configuration
portchannel thash l2thash l2-source-mac-address Enables Layer 2 LAG hashing on the source MAC. **Command mode:** Global configuration
portchannel thash l2thash l2-source-destination-mac Enables Layer 2 LAG hashing on both the source and destination MAC. **Command mode:** Global configuration
show portchannel hash Displays the current LAG hash settings. **Command mode:** All

Layer 3 Link Aggregation Group (LAG) Hash

Layer 3 Link Aggregation Group (LAG) hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 LAG hash parameters for the switch.

Table 240. *Layer 3 LAG Hash Options*

Command Syntax and Usage
portchannel thash l3thash l3-destination-ip-address Enables Layer 3 LAG hashing on the destination IP address. **Command mode:** Global configuration
portchannel thash l3thash l3-source-ip-address Enables Layer 3 LAG hashing on the source IP address. **Command mode:** Global configuration
portchannel thash l3thash l3-source-destination-ip Enables Layer 3 LAG hashing on both the source and the destination IP address. **Command mode:** Global configuration
portchannel thash l3thash l3-use-l2-hash Enables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared. **Command mode:** Global configuration
show portchannel hash Displays the current LAG hash settings. **Command mode:** All

Virtual Link Aggregation Group (vLAG) Configuration

Virtual Link Aggregation Groups (vLAGs) allow you to enhance redundancy and prevent implicit loops without using STP. The vLAG acts as a single virtual entity for the purpose of establishing a multi-port Link Aggregation Group (LAG).

Table 241. *vLAG Configuration Options*

Command Syntax and Usage
`[no] vlag adminkey` *<1-65535>* **`enable`** Enables or disables vLAG on the selected LACP *admin key*. LACP LAGs formed with this *admin key* will be included in the vLAG configuration. **Command mode:** Global configuration
`vlag auto-recovery` *<240-3600>* Sets the duration in seconds of the auto-recovery timer. This timer configures how log after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports. The default value is `300` seconds. **Command mode:** Global configuration
`no vlag auto-recovery` Sets the auto-recovery timer to the default `300` seconds duration. **Command mode:** Global configuration
`[no] vlag enable` Enables or disables vLAG globally. **Command mode:** Global configuration
`[no] vlag mac-address-table refresh` Enables or disables the periodic check of the aging status of synchronized Forwarding Database (FDB) entries. When a MAC address is marked for removal from the FDB table, the entry is reinstalled instead. The default setting is `enabled`. **Note:** This option takes effect only if the aging value for FDB entries is set to 40 seconds or more. For more details on FDB aging, see page 473. **Command mode:** Global configuration
`[no] vlag peer-gateway` Enables or disables the forwarding of packets intended for the switch's vLAG peer. If a packet is received by the switch, but has the MAC address of its vLAG peer, it will be locally forwarded without crossing the vLAG inter-switch link (ISL), thus avoiding the loss of traffic. If the vLAG peer gateway is disabled, packets addressed to the vLAG peer are sent across the ISL and then dropped by the vLAG peer. The default settings is `disabled`. **Note**: The vLAG peer gateway must be configured on both vLAG peers. **Command mode**: Global configuration

Table 241. *vLAG Configuration Options*

Command Syntax and Usage
`[no] vlag portchannel` *<1-72>* **`enable`** Enables or disables vLAG on the selected LAG. **Command mode:** Global configuration
`vlag priority` *<0-65535>* Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch. **Command mode:** Global configuration
`no vlag priority` Resets the vLAG priority of the switch to its default value of `0`. **Command mode:** Global configuration
`vlag startup-delay` *<0-3600>* Sets, in seconds, the vLAG startup delay interval. The default value is `120` seconds. **Command mode:** Global configuration
`no vlag startup-delay` Sets the vLAG startup-delay timer to the default `120` seconds duration. **Command mode:** Global configuration
`vlag tier-id` *<1-512>* Sets the vLAG peer ID. **Command mode:** Global configuration
`no vlag tier-id` Resets the vLAG peer ID to its default value of `0`. **Command mode:** Global configuration
`[no] vlag vrrp active` Enables or disables vLAG VRRP active mode. **Note:** If active mode is disabled, the switch will be in `passive` mode. In `active` mode, Layer 3 traffic is forwarded in all vLAG related VRRP domains. In `passive` mode, Layer 3 traffic is forwarded in a vLAG related VRRP domain only if either the switch or its peer virtual router is the VRRP master. **Command mode:** Global configuration
`show vlag` Displays current vLAG parameters. **Command mode:** All

vLAG Health Check Configuration

These commands enable you to configure a way to check the health status of the vLAG peer.

Table 242. *vLAG Health Check Configuration Options*

Command Syntax and Usage
vlag hlthchk connect-retry-interval *<1-300>* Sets, in seconds, the vLAG health check connect retry interval. The default value is 30 seconds. **Command mode:** Global configuration
no vlag hlthchk connect-retry-interval Resets the vLAG health check connect retry interval to its default value of 30 seconds. **Command mode:** Global configuration
vlag hlthchk keepalive-attempts *<1-24>* Sets the number of vLAG keep alive attempts. The default value is 3. **Command mode:** Global configuration
no vlag hlthchk keepalive-attempts Resets the number of vLAG keep alive attempts to the default value of 3. **Command mode:** Global configuration
vlag hlthchk keepalive-interval *<2-300>* Sets, in seconds, the time between vLAG keep alive attempts. The default value is 5 seconds. **Command mode:** Global configuration
no vlag hlthchk keepalive-interval Resets the time between vLAG keep alive attempts to the default value of 5 seconds. **Command mode:** Global configuration
vlag hlthchk peer-ip {*<IPv4 address>***|***<IPv6 address>***}** Configures the IP address of the peer switch, used for health checks. Use the management IP address of the peer switch. For example: • IPv4 address: 100.20.0.103 • IPv6 address: 3001:0:0:0:0:0:abcd:1234 **Command mode:** Global configuration
no vlag hlthchk peer-ip Deletes the IP address of the peer switch, used for health checks. **Command mode:** Global configuration

vLAG ISL Configuration

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

Table 243. *vLAG ISL Configuration Options*

Command Syntax and Usage
vlag isl adminkey *<1-65535>* Enables vLAG Inter-Switch Link (ISL) on the selected LACP *admin key*. LACP Link Aggregation Groups (LAGs) formed with this *admin key* will be included in the ISL. **Command mode:** Global configuration
no vlag isl adminkey Disables vLAG Inter-Switch Link (ISL) for LACP *admin keys*. **Command mode:** Global configuration
vlag isl portchannel *<1-72>* Enables vLAG Inter-Switch Link (ISL) on the selected LAG. **Command mode:** Global configuration
no vlag isl portchannel Disables vLAG Inter-Switch Link (ISL) for LAGs. **Command mode:** Global configuration
show vlag isl Displays current vLAG Inter-Switch Link (ISL) parameters. **Command mode:** All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G8272.

Table 244. *Link Aggregation Control Protocol Options*

Command Syntax and Usage
`lacp system-priority` *<1-65535>* Defines the priority value for the G8272. Lower numbers provide higher priority. The default value is `32768`. **Command mode:** Global configuration
`default lacp system-priority` Resets the priority value for the switch to its default value of `32768`. **Command mode:** Global configuration
`lacp timeout {short|long}` Defines the timeout period before invalidating LACP data from a remote partner. Choose `short` (3 seconds) or `long` (90 seconds). The default value is `long`. **Note:** To reduce LACPDU processing, use a timeout value of `long`. If your G8272's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static Link Aggregation Groups (LAGs) instead of LACP. **Command mode:** Global configuration
`default lacp timeout` Resets the timeout period before invalidating LACP data from a remote partner to its default value of `long`. **Command mode:** Global configuration
`default lacp` Resets the LACP system configuration to its default values. **Command mode:** Global configuration
`portchannel` *<73-144>* **`lacp key`** *<1-65535>* Enables a static LACP LAG. In this mode, ports sharing the same LACP admin key can form a single LAG, with the specified LAG ID. The active LAG is picked based on the ports which occupy first the LAG ID. Member ports that cannot join this LAG are prohibited from forming secondary LACP groups. Instead, they are set in a suspended state where they discard all non-LACP traffic. **Command mode:** Global configuration
`no portchannel` *<73-144>* Deletes a static LACP LAG. **Command mode:** Global configuration

Table 244. *Link Aggregation Control Protocol Options*

Command Syntax and Usage
`no lacp` *<1-65535>* Deletes a selected LACP LAG, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key.* **Command mode:** Global configuration
`show lacp` Display current LACP configuration. **Command mode:** All

LACP Port Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the selected port.

Table 245. *LACP Port Options*

Command Syntax and Usage
`lacp key` *<1-65535>* Set the *admin key* for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP LAG group. **Command mode:** Interface port/Interface portchannel
`default lacp key` Resets the LACP admin key of the port to the default value. **Command mode:** Interface port/Interface portchannel
`lacp mode {off|active|passive}` Set the LACP mode for this port, as follows: o `off` turns LACP off for this port. You can use this port to manually configure a static LAG. o `active` turns LACP on and set this port to active. Active ports initiate LACPDUs. o `passive` turns LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. The default value is `off`. **Command mode:** Interface port/Interface portchannel
`default lacp mode` Resets the LACP mode of the port to its default value. **Command mode:** Interface port/Interface portchannel

Table 245. *LACP Port Options*

Command Syntax and Usage
lacp priority *<1-65535>* Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Interface port/Interface portchannel
default lacp priority Resets the priority value for the port to its default value of 32768. **Command mode:** Interface port/Interface portchannel
lacp suspend-individual Sets the port in LACP suspended state if it does not receive LACPDUs anymore. **Note:** The default value is suspended for all switch ports. **Command mode:** Interface port/Interface portchannel
no lacp suspend-individual Sets the port in LACP individual state if it does not receive LACPDUs anymore. **Command mode:** Interface port/Interface portchannel
default lacp suspend-individual Resets the LACP state of the port to its default value. **Command mode:** Interface port/Interface portchannel
default lacp Resets the LACP port configuration to its default values. **Command mode:** Interface port/Interface portchannel
port-channel min-links *<1-32>* Set the minimum number of links for the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the LAG is placed in the down state. **Command mode:** Interface port/Interface portchannel
default port-channel min-links Restores the minimum number of links for this port to its default value. **Command mode:** Interface port/Interface portchannel
show interface port *<port alias or number>* **lacp** Displays the current LACP configuration for this port. **Command mode:** All

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see "High Availability" in the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Table 246. *Layer 2 Failover Configuration Options*

Command Syntax and Usage
[no] failover enable Globally enables or disables Layer 2 Failover. **Command mode:** Global configuration
show failover trigger Displays current Layer 2 Failover parameters. **Command mode:** All

Failover Trigger Configuration

The following table describes the Failover Trigger commands.

Table 247. *Failover Trigger Configuration Options*

Command Syntax and Usage
[no] failover trigger *<1-8>* **enable** Enables or disables the Failover trigger. **Command mode:** Global configuration
failover trigger *<1-8>* **limit** *<0-1024>* Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. **Command mode:** Global configuration
no failover trigger *<1-8>* Deletes the Failover trigger. **Command mode:** Global configuration
show failover trigger *<1-8>* Displays the current failover trigger settings. **Command mode:** All

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts any non-management port.

Table 248. *Failover Manual Monitor Port Options*

Command Syntax and Usage
[no] failover trigger *<1-8>* **mmon monitor adminkey** *<1-65535>* Adds or removes an LACP *admin key* to the Manual Monitor Port configuration. LACP Link Aggregation Groups (LAGs) formed with this admin key will be included in the Manual Monitor Port configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon monitor member** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Port configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon monitor portchannel** *<1-72>* Adds or removes the selected LAG to the Manual Monitor Port configuration. **Command mode:** Global configuration
show failover trigger *<1-8>* Displays the current Failover settings. **Command mode:** All

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts any non-management port.

Table 249. *Failover Manual Monitor Control Options*

Command Syntax and Usage
[no] failover trigger *<1-8>* **mmon control adminkey** *<1-65535>* Adds or removes an LACP *admin key* to the Manual Monitor Control configuration. LACP Link Aggregation Groups (LAGs) formed with this admin key will be included in the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control member** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control portchannel** *<1-72>* Adds or removes the selected LAG to the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control vmember** *<virtual port number>* Adds or removes the specified virtual port to the Manual Monitor Control configuration. **Command mode:** Global configuration
show failover trigger *<1-8>* Displays the current Failover settings. **Command mode:** All

Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see "Hot Links" in the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Table 250. *Hot Links Configuration Options*

Command Syntax and Usage
`[no] hotlinks bpdu` Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned `off`. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time). The default setting is `disabled`. **Command mode:** Global configuration
`[no] hotlinks enable` Globally enables or disables Hot Links. **Command mode:** Global configuration
`[no] hotlinks fdb-update` Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface. The default value is `disabled`. **Command mode:** Global configuration
`hotlinks fdb-update-rate` *<10-1000>* Configures the FDB Update rate in packets per second. **Command mode:** Global configuration
`show hotlinks` Displays current Hot Links parameters. **Command mode:** All

Hot Links Trigger Configuration

The following table describes the Hot Links Trigger commands.

Table 251. *Hot Links Trigger Configuration Options*

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* **enable** Enables or disables the Hot Links trigger. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **forward-delay** *<0-3600>* Configures the Forward Delay interval, in seconds. The default value is **1** second. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **name** *<1-32 characters>* Defines a name for the Hot Links trigger. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **name** Removes the name of the specified Hot Links trigger. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **preemption** Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is **enabled**. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* Deletes the Hot Links trigger. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Master Configuration

Use the following commands to configure the Hot Links Master interface.

Table 252. *Hot Links Master Configuration Options*

Command Syntax and Usage
hotlinks trigger *<1-25>* **master adminkey** *<1-65535>* Adds an LACP *admin key* to the Master interface. LACP Link Aggregation Groups (LAGs) formed with this *admin key* will be included in the Master interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **master adminkey** Clears all LACP *admin keys* on the Master interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **master port** *<port alias or number>* Adds the selected port to the Hot Links Master interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **master port** Clears all ports added to the Hot Links Master interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **master portchannel** *<1-72>* Adds the selected LAG to the Hot Links Master interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **master portchannel** Clears all LAGs added to the Hot Links Master interface. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

Table 253. *Hot Links Backup Configuration Options*

Command Syntax and Usage
hotlinks trigger *<1-25>* **backup adminkey** *<1-65535>* Adds an LACP *admin key* to the Hot Links Backup interface. LACP Link Aggregation Groups (LAGs) formed with this *admin key* will be included in the Hot Links Backup interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **backup adminkey** Clears all LACP *admin keys* on the Hot Links Backup interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **backup port** *<port alias or number>* Adds the selected port to the Hot Links Backup interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **backup port** Clears all ports added to the Hot Links Backup interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **backup portchannel** *<1-72>* Adds the selected LAG to the Hot Links Backup interface. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **backup portchannel** Clears all LAGs added to the Hot Links Backup interface. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

VLAN Configuration

These commands configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, VLAN 1 is the only VLAN configured on the switch. All ports are members of VLAN 1 by default. Up to 4095 VLANs can be configured on the G8272.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 254. *VLAN Configuration Options*

Command Syntax and Usage
vlan *<VLAN ID (1-4094)>* Enter VLAN configuration mode. If the specified VLAN(s) doesn't exist, it will be created. **Command mode:** Global configuration
name *<1-32 characters>* Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. **Command mode:** VLAN
no name Removes the assigned name from the current VLAN. **Command mode:** VLAN
protocol-vlan *<protocol number (1-8)>* Configures the Protocol-based VLAN (PVLAN). For command options, see page 502. **Command mode:** VLAN
shutdown Disables local traffic on the specified VLAN. The default setting is `enabled` (**no shutdown**). **Command mode:** VLAN
no shutdown Enables local traffic on the specified VLAN. This is the default setting. **Command mode:** VLAN
stg *<1-256>* Assigns a VLAN to a Spanning Tree Group. **Note**: For MST no VLAN assignation is required. VLANs are mapped from CIST. **Command mode:** VLAN

Table 254. *VLAN Configuration Options*

Command Syntax and Usage
[no] vmap *<1-128>* **[serverports|non-serverports]** Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to server ports only or non-server ports only. If you do not select a port type, the VMAP is applied to the entire VLAN. **Command mode:** VLAN
no vlan *<VLAN ID (1-4094)>* Deletes the specified VLAN. **Command mode:** Global configuration
show vlan information Displays the current VLAN configuration. **Command mode:** All

Note: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

Protocol-Based VLAN Configuration

Use the following commands to configure Protocol-based VLAN for the selected VLAN.

Table 255. *Protocol VLAN Configuration Options*

Command Syntax and Usage
[no] protocol-vlan *<protocol number (1-8)>* **enable** Enables or disables the selected protocol on the VLAN. **Command mode:** VLAN
protocol-vlan *<protocol number (1-8)>* **frame-type {ether2|llc|snap}** *<ethernet type>* Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as `0080` (IPv4). **Command mode:** VLAN
[no] protocol-vlan *<protocol number (1-8)>* **member** *<port alias or number>* Adds or removes a port to the selected PVLAN. **Command mode:** VLAN
protocol-vlan *<protocol number (1-8)>* **priority** *<0-7>* Configures the priority value for this PVLAN. **Command mode:** VLAN

Table 255. *Protocol VLAN Configuration Options (continued)*

Command Syntax and Usage
protocol-vlan *<protocol number (1-8)>* **protocol** *<protocol type>* Selects a pre-defined protocol, as follows: o decEther2: DEC Local Area Transport o ipv4Ether2: Internet IP (IPv4) o ipv6Ether2: IPv6 o ipx802.2: Novell IPX 802.2 o ipx802.3: Novell IPX 802.3 o ipxEther2: Novell IPX o ipxSnap: Novell IPX SNAP o netbios: NetBIOS 802.2 o rarpEther2: Reverse ARP o sna802.2: SNA 802.2 o snaEther2: IBM SNA Service on Ethernet o vinesEther2: Banyan VINES o xnsEther2: XNS Compatibility **Command mode:** VLAN
[no] protocol-vlan *<protocol number (1-8)>* **tag-pvlan** *<port alias or number>* Adds or removes a port that will be tagged by the selected protocol on this VLAN. **Command mode:** VLAN
no protocol-vlan *<protocol number (1-8)>* Deletes the selected protocol configuration from the VLAN. **Command mode:** VLAN
show protocol-vlan *<protocol number (1-8)>* Displays current parameters for the selected PVLAN. **Command mode:** All

Private VLAN Configuration

Use the following commands to configure Private VLANs.

Table 256. *Private VLAN Options*

Command Syntax and Usage
`private-vlan association [add|remove]` *<secondary VLAN list>* Configures Private VLAN mapping between a primary VLAN and secondary VLANs. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise: o `add` appends the secondary VLANs to the ones currently associated o `remove` excludes the secondary VLANs from the ones currently associated **Command mode:** VLAN
`[no] private-vlan community` Enables or disables the VLAN type as a community VLAN. Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs. **Command mode:** VLAN
`[no] private-vlan isolated` Enables or disables the VLAN type as an isolated VLAN. The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. **Command mode:** VLAN
`[no] private-vlan primary` Enables or disables the VLAN type as a Primary VLAN. A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN. **Command mode:** VLAN
`show vlan private-vlan [type]` Displays current parameters for the selected Private VLAN(s). o `type` lists only the VLAN type for each private VLAN: community, isolated, or primary **Command mode:** All

Flooding VLAN Configuration Menu

The following table describes the Flooding VLAN commands.

Table 257. *Flooding VLAN Menu Options*

Command Syntax and Usage
`[no] flood` Enables or disables the switch to flood unregistered IP multicast traffic to all ports. The default setting is `enabled`. **Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must enable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group. **Command mode**: VLAN
`[no] cpu` Enables or disables the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: o If no Mrouter is present, drop subsequent packets with same IPMC. o If a Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is `enabled`. **Note**: If both `flood` and `cpu` are disabled, the switch drops all unregistered IPMC traffic. **Command mode**: VLAN
`[no] optflood` Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is `disabled`. **Command mode**: VLAN
`show vlan` *<VLAN ID (1-4094)>* **`information`** Displays the current flooding parameters for the selected VLAN. **Command mode**: All

Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 258. *Layer 3 Configuration Commands*

Command Syntax and Usage
`interface ip` *<1-128>* Configures the IP Interface. The G8272 supports up to 128 IP interfaces. To view command options, see page 508. **Command mode:** Global configuration
`ip pim component` *<1-2>* Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see page 616. **Command mode:** Global configuration
`ip router-id` *<IP address>* Sets the router ID. **Command mode:** Global configuration
`no ip router-id` Removes the router ID. **Command mode:** Global configuration
`route-map` *<1-255>* Enters IP Route Map mode. To view command options, see page 527. **Command mode:** Global configuration
`router bgp` Enters Border Gateway Protocol (BGP) configuration mode. To view command options, see page 565. **Command mode:** Global configuration
`router ospf` Enters OSPF configuration mode. To view command options, see page 538. **Command mode:** Global configuration
`ipv6 router ospf` Enters OSPFv3 configuration mode. To view command options, see page 548. **Command mode:** Global configuration
`router rip` Enters the Routing Interface Protocol (RIP) configuration mode. To view command options, see page 534. **Command mode:** Global configuration

Table 258. *Layer 3 Configuration Commands (continued)*

Command Syntax and Usage
router vrrp Enters Virtual Router Redundancy (VRRP) configuration mode. To view command options, see page 604. **Command mode:** Global configuration
show ip information Displays all IP information. **Command mode:** All
show layer3 Dumps all Layer 3 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data before issuing the dump commands. **Command mode:** All

IP Interface Configuration

The G8272 supports up to 128 IP interfaces. Each IP interface represents the switch on an IP subnet on your network.

Interface 127 and interface 128 are reserved for switch management.

The interface option is `disabled` by default.

Table 259. *IP Interface Configuration Options*

Command Syntax and Usage
`interface ip` *<1-128>* Enter IP interface mode. **Command mode:** Global configuration
`[no] enable` Enables or disables this IP interface. **Command mode:** Interface IP
`ip address` *<IP address>* **`[`***<IP netmask>***`] [enable]`** Configures the IP address of the switch interface, using dotted decimal notation. The `enable` option also enables the IP interface. **Command mode:** Interface IP
`ip netmask` *<IP netmask>* Configures the IP subnet address mask for the interface, using dotted decimal notation. **Command mode:** Interface IP
`ipv6 address` *<IPv6 address>* **`[`***<IPv6 prefix length>* **`[anycast]] [enable]`** Configures the IPv6 address of the switch interface, using hexadecimal format with colons. The `anycast` option configures the IPv6 address as an IPv6 anycast address. The `enable` option also enables the IP interface. **Command mode:** Interface IP
`ipv6 prefixlen` *<IPv6 prefix length (1-128)>* Configures the subnet IPv6 prefix length. The default value is `0` (zero). **Command mode:** Interface IP
`ipv6 secaddr6 address` *<IPv6 address> <IPv6 prefix length>* **`[anycast]`** Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons. The `anycast` option configures the secondary IPv6 address as an IPv6 anycast address. **Command mode:** Interface IP
`no ipv6 secaddr6 address` Removes the secondary IPv6 address. **Command mode:** Global configuration

Table 259. *IP Interface Configuration Options (continued)*

Command Syntax and Usage
[no] ipv6 unreachables Enables or disables sending of ICMP Unreachable messages. The default setting is `enabled`. **Command mode:** Interface IP
[no] ip6host Enables or disables the IPv6 Host Mode on this interface. The default setting is `disabled` for data interfaces, and `enabled` for the management interface. **Command mode:** Interface IP
[no] relay Enables or disables the BOOTP relay on this interface. The default setting is `enabled`. **Command mode:** Interface IP
tenant services tenant-id *<1-30>* Defines the tenants who use the interface to access a service network. Up to 4 services per tenant are supported. **Command mode**: Interface IP
no tenant services tenant-id [*<1-30>***]** Removes tenants who use the interface to access a service network. **Command mode**: Interface IP
tenant tenant-id *<1-30>* Defines the tenant downlink network. Up to 10 subnets per tenant are supported. **Command mode**: Interface IP
no tenant tenant-id [*<1-30>***]** Removes all tenant or a specific tenant from the current interface. **Command mode**: Interface IP
tenant uplink tenant-id *<1-30>* **[active|stanby]** Defines the tenants who use this interface as an uplink interface. Up to 2 uplinks per tenant are supported. **Command mode**: Interface IP
no tenant uplink tenant-id [*<1-30>***]** Removes the tenants who use the current interface as an uplink interface. **Command mode:** Interface IP

Table 259. *IP Interface Configuration Options (continued)*

Command Syntax and Usage
vlan *<VLAN ID (1-4094)>* Configures the VLAN number for this interface. Each interface can belong to one VLAN. **IPv4**: Each VLAN can contain multiple IPv4 interfaces. **IPv6**: Each VLAN can contain only one IPv6 interface. **Note**: Assigning VLANs only applies to in-band management IP interfaces 1 and 2. Default is VLAN 1 if not configured. **Command mode:** Interface IP
no interface ip *<1-128>* Removes this IP interface. **Command mode:** Global configuration
show ip tenant [*<1-30>***]** Displays tenant information. **Command mode**: All
show ip tenant info [*<1-30>***]** Displays tenant dynamic ACLs, including next-hops. **Command mode**: All
show interface ip [*<1-128>***]** Displays the current interface settings. **Command mode:** All

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery configuration commands.

Table 260. *IPv6 Neighbor Discovery Configuration Options*

Command Syntax and Usage
`[no] ipv6 nd advmtu` Enables or disables the MTU option in Router Advertisements. The default setting is `enabled`. **Command mode:** Interface IP
`ipv6 nd dad-attempts` *<1-10>* Configures the maximum number of duplicate address detection attempts. The default value is `1`. **Command mode:** Interface IP
`no ipv6 nd dad-attempts` Resets the maximum number of duplicate address detection attempts to the default value of `1`. Command mode: Interface IP
`ipv6 nd hops-limit` *<0-255>* Configures the Router Advertisement hop limit. The default value is `64` hops. **Command mode:** Interface IP
`no ipv6 nd hops-limit` Resets the IPv6 Router Advertisement hop limit to its default value of `64` hops. Command mode: Interface IP
`[no] ipv6 nd managed-config` Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default setting is `disabled`. **Command mode:** Interface IP
`[no] ipv6 nd other-config` Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is `disabled`. **Command mode:** Interface IP

Table 260. *IPv6 Neighbor Discovery Configuration Options (continued)*

Command Syntax and Usage
ipv6 nd ra-interval *<4-1800>* Configures the Router Advertisement maximum interval. The default value is `600` seconds. **Note**: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval. **Command mode:** Interface IP
no ipv6 nd ra-interval Resets the IPv6 Router Advertisement maximum interval to its default value of `600` seconds. **Command mode:** Interface IP
ipv6 nd ra-intervalmin *<3-1350>* Configures the Router Advertisement minimum interval. The default value is `198` seconds. **Note**: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval. **Command mode:** Interface IP
no ipv6 nd ra-intervalmin Resets the IPv6 Router Advertisement minimum interval to its default value of `198` seconds. **Command mode:** Interface IP
ipv6 nd ra-lifetime *<0-9000>* Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (`advint`). The default value is `1800` seconds. **Command mode:** Interface IP
no ipv6 nd ra-lifetime Resets the IPv6 Router Advertisement lifetime interval to its default value of `1800` seconds. **Command mode:** Interface IP
ipv6 nd reachable-time *<1-3600>* **ipv6 nd reachable-time** *<1-3600000>* **ms** Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is `30` seconds. **Command mode:** Interface IP
no ipv6 nd reachable-time Resets the advertised reachability time to its default value of `30` seconds. **Command mode:** Interface IP

Table 260. *IPv6 Neighbor Discovery Configuration Options (continued)*

Command Syntax and Usage
ipv6 nd retransmit-time *<0-4294967>* **ipv6 nd retransmit-time** *<0-4294967295>* **ms** Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is `1` second. **Command mode:** Interface IP
no ipv6 nd retransmit-time Resets the Router Advertisement re-transmit timer to its default value of `1` second. Command mode: Interface IP
[no] ipv6 nd suppress-ra Enables or disables IPv6 Router Advertisements on the interface. The default setting is `disabled` (suppress Router Advertisements). **Command mode:** Interface IP

Default Gateway Configuration

The switch can be configured with up to four IPv4 gateways, as follows:

- Gateway 1, 2 and 3: data traffic
- Gateway 4: management traffic for interface 128

This option is `disabled` by default.

Table 261. *IPv4 Default Gateway Options*

Command Syntax and Usage
ip gateway *<1-4>* **address** *<IP address>* **[enable]** Configures the IP address of the default IP gateway using dotted decimal notation. The `enable` option also enables the IP gateway. **Command mode:** Global configuration
[no] ip gateway *<1-4>* **arp-health-check** Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is `disabled`. **Note:** The `arp` option does not apply to management gateways. **Command mode:** Global configuration
[no] ip gateway *<1-4>* **enable** Enables or disables the gateway for use. **Command mode:** Global configuration
ip gateway *<1-4>* **interval** *<0-60>* The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds and the default is `2` seconds. **Command mode:** Global configuration
ip gateway *<1-4>* **retry** *<1-120>* Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts and the default is `8` attempts. **Command mode:** Global configuration
no ip gateway *<1-4>* Deletes the gateway from the configuration. **Command mode:** Global configuration
show ip gateway *<1-4>* Displays the current gateway settings. **Command mode:** All

IPv4 Static Route Configuration

Up to 128 IPv4 static routes can be configured.

Table 262. *IPv4 Static Route Configuration Options*

Command Syntax and Usage
ip route *<IP subnet> <IP netmask> <IP nexthop>* **[***<IP interface number>***||port** *<port alias or number>***]** Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation. **Command mode:** Global configuration
no ip route *<IP subnet> <IP netmask>* **[***<IP interface number>***|***<IP nexthop>**[***<IP interface number>***]||port** *<port alias or number>***]** Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation. **Command mode:** Global configuration
ip route ecmphash [dipsip|sip] Configures ECMP hashing parameters. You may choose one or more of the following parameters: o `dipsip`: Destination IP and source IP address o `sip`: Source IP address **Command mode:** Global configuration
[no] ip route healthcheck Enables or disables static route health checks. The default setting is `disabled`. **Command mode:** Global configuration
ip route interval *<1-60>* Configures the ECMP health-check ping interval, in seconds. The default value is `1` second. **Command mode:** Global configuration
ip route retries *<1-60>* Configures the number of ECMP health-check retries. The default value is `3` retries. **Command mode:** Global configuration
no ip route all Clears all IP statis routes. **Command mode:** Global configuration

Table 262. *IPv4 Static Route Configuration Options (continued)*

Command Syntax and Usage
no ip route destination-address *<IP address>* Clears all IP static routes with this destination. **Command mode:** Global configuration
no ip route gateway *<IP address>* Clears all IP static routes that use this gateway. **Command mode:** Global configuration
no ip route interface *<IP interface number>* Clears all IP static routes that use the specified IP interface. **Command mode:** Global configuration
no ip route port *<port alias or number>* Clears all IP static routes that use the specified port. **Command mode:** Global configuration
show ip route static Displays the current IP static routes. **Command mode:** All

IP Multicast Route Configuration

The following table describes the IP Multicast (IPMC) route commands.

Note: Before you can add an IPMC route, IGMP must be turned on, IGMP Snooping/Relay must be enabled, and the required VLANs must be added to IGMP Snooping/Relay.

Table 263. *IP Multicast Route Configuration Commands*

Command Syntax and Usage
[no] ip mroute *<IPMC destination> <VLAN ID (1-4094)> <port alias or number>* **[{primary|backup|host} [***<virtual router ID>***]]** Adds or removes a static multicast route. The destination address, VLAN and member port of the route must be specified. **Command mode:** Global configuration
[no] ip mroute *<IP address> <VLAN ID (1-4094)>* **portchannel** *<1-72>* **[{primary|backup|host} [***<virtual router ID>***]]** Adds or removes a static multicast route. The destination address, VLAN, and member Link Aggregation Group (LAG) of the route must be specified. **Command mode:** Global configuration
[no] ip mroute *<IP address> <VLAN ID (1-4094)>* **adminkey** *<1-65535>* **[{primary|backup|host} [***<virtual router ID>***]]** Adds or removes a static multicast route. The destination address, VLAN, and LACP *admin key* of the route must be specified. **Command mode:** Global configuration
no ip mroute all Removes all the static multicast routes configured. **Command mode:** Global configuration
show ip mroute Displays the current IP multicast routes. **Command mode:** All

ARP Configuration

Address Resolution Protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

Table 264. *ARP Configuration Options*

Command Syntax and Usage
ip arp rearp *<2-120>* Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache. The default value is 5 minutes. **Command mode:** Global configuration
show [ip] arp Displays the current ARP configurations. **Command mode:** All

ARP Local Proxy Configuration

By using ARP local proxy feature, the router mediates the ARP traffic performed within a subnet. Each ARP request is received by the router. In response, the router sends its own MAC address. Any traffic between hosts is forwarded via the router's layer 3 interface.

Note: For a routed interface, enabling ARP local proxy feature requires disabling all ICMP redirects.

Table 265. *ARP Local Proxy Configuration Options*

Command Syntax and Usage
[no] ip local-proxy-arp Enables or disables the ARP local proxy. **Command mode:** Interface IP/Interface Port
show interface ip [*<1-128>***]** Displays the current interface settings. **Command mode**: All

ARP Static Configuration

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

Table 266. *ARP Static Configuration Options*

Command Syntax and Usage
ip arp *<IP address>* *<MAC address>* **[vlan** *< VLAN ID (1-4094)>***]** **[port** *<port alias or number>***]** Adds a permanent ARP entry. To enable ARP on a LAG, add the port number of a member of the LAG. **Command mode:** Global configuration
ip arp *<destination unicast IP address>* *<destination multicast MAC address>* **vlan** *<cluster vlan number>* Adds a static multicast ARP entry for Network Load Balancing (NLB). **Command mode:** Global configuration
no ip arp *<IP address>* Deletes a permanent ARP entry. **Command mode:** Global configuration
no ip arp all [ip *<IP interface number>***|interface port** *<port alias or number>***|vlan** *<VLAN ID (1-4094)>***]** Deletes all static ARP entries or just the ARP entries that use a specific IP interface, port or vlan. **Command mode:** Global configuration
show [ip] arp static Displays current static ARP configuration. **Command mode:** All

Dynamic ARP Inspection Configuration

Dynamic ARP Inspection (DAI) is a security feature that enables the device to intercept and examine all ARP request and response packets in a subnet and discard those packets with invalid IP to MAC address bindings.

DAI uses information gathered by DHCP Snooping to validate ARP information that travels through ports marked as being not trusted.

Table 267. *Dynamic ARP Inspection Configuration Options*

Command Syntax and Usage
`[no] ip arp inspection vlan` *<VLAN ID (1-4094)>* Enables or disables DAI on the selected VLANs. **Command mode:** Global configuration
`[no] ip arp inspection trust` Configures the current port to be a DAI trusted port. On a DAI trusted port, all ARP packets skip the security check. The default settings is `untrusted`. **Note:** Configuring trusted interfaces as being untrusted can result in a loss of connectivity. **Command mode:** Interface port
`[no] logging log arp-inspection` Enables or disables logging for DAI. The default setting is `enabled`. **Command mode:** Global configuration
`show ip arp inspection` Displays the current DAI configuration settings. For mode details, see page 93. **Command mode:** All

IP Forwarding Configuration

The following table describes the IP Forwarding commands.

Table 268. *IP Forwarding Configuration Options*

Command Syntax and Usage
[no] ip routing Enables or disables IP forwarding (routing) on the G8272. Forwarding is turned `on` by default. **Command mode:** Global configuration
[no] ip routing directed-broadcasts Enables or disables forwarding directed broadcasts. The default setting is `disabled`. **Command mode:** Global configuration
[no] ip routing icmp6-redirect Enables or disables IPv6 ICMP re-directs. The default setting is `disabled`. **Command mode:** Global configuration
[no] ip routing no-icmp-redirect Enables or disables ICMP re-directs. The default setting is `disabled`. **Command mode:** Global configuration
show ip routing Displays the current IP forwarding settings. **Command mode:** All

Network Address Translation Configuration

Network Address Translation (NAT) is a mechanism through which IP addresses are mapped from one realm to another in order to provide transparent routing to hosts. For more information about NAT, please refer to *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Table 269. *NAT Configuration Options*

Command Syntax and Usage
[no] ip nat enable Enables or disables NAT feature. The default setting is `disabled`. **Command mode:** Global configuration
[no] ip nat inside destination static *<outside local IP address> <outside global IP address>* **[one-way]** Configures one-to-one translations of the outside local address to the outside global address. The `one-way` option restricts the NAT process to only translating local IP addresses to global IP addresses. **Command mode:** Global configuration
[no] ip nat inside destination static {tcp|udp} *<outside local IP address> <local TCP/UDP port number> <outside global IP address> <global TCP/UDP port number>* **[one-way]** Configures one-to-one translations of the outside local address and local TCP/UDP port number to the outside global address and global TCP/UDP port number. The `one-way` option restricts the NAT process to only translating local IP addresses to global IP addresses. **Command mode:** Global configuration
[no] ip nat inside source pool *<pool name>* **pool** *<translation pool name>* **[overload] [one-way]** Configures a mapping of multiple inside local IP addresses to multiple inside global IP addresses. The `overload` option maps multiple local IP addresses to a single global IP address. The `one-way` option restricts the NAT process to only translating local IP addresses to global IP addresses. **Command mode:** Global configuration
[no] ip nat inside source static *<inside local IP address> <inside global IP address>* **[one-way]** Configures one-to-one translations of the inside local address to the inside global address. The `one-way` option restricts the NAT process to only translating local IP addresses to global IP addresses. **Command mode:** Global configuration

Table 269. *NAT Configuration Options*

Command Syntax and Usage
[no] ip nat inside source static {tcp|udp} *<inside local IP address> <local TCP/UDP port number> <inside global IP address> <global TCP/UDP port number>* **[one-way]** Configures one-to-one translations of the inside local address and local TCP/UDP port number to the inside global address and global TCP/UDP port number. The `one-way` option restricts the NAT process to only translating local IP addresses to global IP addresses. **Command mode:** Global configuration
[no] ip nat outside destination static *<inside global IP address> <inside local IP address>* **[one-way]** Configures one-to-one translations of the inside global address to the inside local address. The `one-way` option restricts the NAT process to only translating global IP addresses to local IP addresses. **Command mode:** Global configuration
[no] ip nat outside destination static {tcp|udp} *<inside global IP address> <global TCP/UDP port number> <inside local IP address> <local TCP/UDP port number>* **[one-way]** Configures one-to-one translations of the inside global address and global TCP/UDP port number to the inside local address and local TCP/UDP port number. The `one-way` option restricts the NAT process to only translating global IP addresses to local IP addresses. **Command mode:** Global configuration
[no] ip nat outside source pool *<pool name>* **pool** *<translation pool name>* **[overload] [one-way]** Configures a mapping of multiple outside global IP addresses to multiple outside local IP addresses. The `overload` option maps multiple local IP addresses to a single global IP address. The `one-way` option restricts the NAT process to only translating global IP addresses to local IP addresses. **Command mode:** Global configuration
[no] ip nat outside source static *<outside global IP address> <outside local IP address>* **[one-way]** Configures one-to-one translations of the outside global address to the outside local address. The `one-way` option restricts the NAT process to only translating global IP addresses to local IP addresses. **Command mode:** Global configuration

Table 269. *NAT Configuration Options*

Command Syntax and Usage
[no] ip nat outside source static {tcp|udp} *<outside global IP address> <global TCP/UDP port number> <outside local IP address> <local TCP/UDP port number>* **[one-way]** Configures one-to-one translations of the outside global address and global TCP/UDP port number to the outside local address and local TCP/UDP port number. The `one-way` option restricts the NAT process to only translating global IP addresses to local IP addresses. **Command mode:** Global configuration
ip nat pool *<pool name> <start IP address> <end IP address>* **netmask** *<IP netmask>* **[port-range** *<start port> <end port>***]** Configures a NAT pool. A maximum number of `1000` pools can be configured. **Command mode:** Global configuration
no ip nat pool *<pool name>* Deletes the specified NAT pool. **Command mode:** Global configuration
no ip nat pools Deletes all NAT pools. **Command mode:** Global configuration
[no] ip nat proxy-arp enable Enables or disables NAT proxy arp. **Command mode:** Global configuration
ip nat translation timeout *<0-4294967>* Configures a timeout period for dynamic NAT translations. The default value is `300` seconds. **Command mode:** Global configuration
no ip nat translation timeout Resets the timeout period for dynamic NAT translations to its default value of `300` seconds. **Command mode:** Global configuration
no ip nat {all|static|dynamic} Deletes an entire category of configured translations. **Command mode:** Global configuration
[no] ip nat {inside|outside} Configures a specific IP interface to be part of inside/outside realm. Use the `no` form to move the IP interface back to default realm. **Command mode:** Interface IP

Table 269. *NAT Configuration Options*

Command Syntax and Usage
ip nat default Configures a specific IP interface to be part of default realm. **Command mode:** Interface IP
show ip nat Displays the current NAT configuration. **Command mode:** All
show ip nat translations Displays the current NAT table. Command mode: All

Network Filter Configuration

The following table describes the Network Filter commands.

Table 270. *IP Network Filter Configuration Options*

Command Syntax and Usage
ip match-address *<1-256> <IP address> <IP netmask>* Sets the starting IP address and IP Netmask for this filter to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default address is `0.0.0.0 0.0.0.0.` **Command mode:** Global configuration.
[no] ip match-address *<1-256>* **enable** Enables or disables the Network Filter configuration. **Command mode:** Global configuration
no ip match-address *<1-256>* Deletes the Network Filter configuration. **Command mode:** Global configuration
show ip match-address [*<1-256>***]** Displays the current the Network Filter configuration. **Command mode:** All

Routing Map Configuration

Routing maps control and modify routing information.

Note: The *map number (1-255)* represents the routing map you wish to configure.

Table 271. *Routing Map Configuration Options*

Command Syntax and Usage
route-map *<1-255>* Enter route map configuration mode. **Command mode:** Global configuration
access-list *<1-32>* Configures the Access List. For more information, see page 530. **Command mode:** Route map
as-path-list *<1-8>* Configures the Autonomous System (AS) Filter. For more information, see page 533. **Command mode:** Route map
as-path-preference *<1-65535>* Sets the AS path preference of the matched route. You can configure up to 32 path preferences. **Command mode:** Route map
no as-path-preference Removes the AS path preference of the current route map. **Command mode:** Route map
[no] enable Enables or disables the route map. **Command mode:** Route map
local-preference *<0-4294967294>* Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred. **Command mode:** Route map
no local-preference Removes the local preference of the current route map. **Command mode:** Route map
metric *<1-4294967294>* Sets the metric of the matched route. **Command mode:** Route map

Table 271. *Routing Map Configuration Options (continued)*

Command Syntax and Usage
no metric Removes the configured metric of the current route map. **Command mode:** Route map
metric-type {1|2} Assigns the type of OSPF metric. o Type 1—External routes are calculated using both internal and external metrics. o Type 2—External routes are calculated using only the external metrics. Type 1 routes are preffered over Type 2. The default is Type 1. **Command mode:** Route map
no metric-type Removes the OSPF metric of the current route map. **Command mode:** Route map
precedence *<1-255>* Sets the precedence of the route map. The smaller the value, the higher the precedence. The default value is 10. **Command mode:** Route map
set community [<*community string*>**|none]** Sets the BGP community attribute. Enter up to 32 communities strings using the format, aa:nn. For example, 12:34. Valid strings are from 0:0 to 65535:65535. The none option removes the community attribute from prefix that passed the route-map. **Command mode:** Route map
no set community Removes the BGP community attribute from the route map configuration. **Command mode:** Route map
weight *<0-65534>* Sets the weight of the route map. **Command mode:** Route map
no weight Deletes the weight of the current route map. **Command mode:** Route map

Table 271. *Routing Map Configuration Options (continued)*

Command Syntax and Usage
no route-map *<1-255>* Deletes the route map. **Command mode:** Global configuration
show route-map [*<1-255>***]** Displays the current route configuration. **Command mode:** All

IP Access List Configuration

Use the following commands to configure an access list statement on the current route-map.

Note: The *access list number* (1-32) represents the IP access list you wish to configure.

Table 272. *IP Access List Configuration Options*

Command Syntax and Usage
access-list *<1-32>* **action {permit|deny}** Permits or denies action for the access list. **Command mode:** Route map
[no] access-list *<1-32>* **enable** Enables or disables the access list. **Command mode:** Route map
[no] access-list *<1-32>* **match-access-control** *<1-256>* Sets the network filter number. **Command mode:** Route map
[no] access-list *<1-32>* **match-address** *<1-256>* Sets the network filter number. See "Network Filter Configuration" on page 526 for details. **Command mode:** Route map
access-list *<1-32>* **metric** *<1-4294967294>* Sets the metric value in the AS-External (ASE) LSA. **Command mode:** Route map
no access-list *<1-32>* **metric** Removes the current metric value for the specified access list. **Command mode:** Route map
no access-list *<1-32>* Deletes the access list. **Command mode:** Route map
show route-map *<1-255>* **access-list** *<1-32>* Displays the current Access List configuration. **Command mode:** All

Policy-Based Routing Configuration

Use the following commands to set up policy-based routing.

Note: Multiple access lists can be entered separated by a comma (for example, "2,5,17"); a range of access lists can be entered using a hyphen (such as "2-23").

Table 273. *IP Next Hop Configuration Options*

Command Syntax and Usage
[no] set ip dscp *<0-63>* **[access-list** *<1-32>***]** Sets the IP DSCP value in the IP header for packets that match route map policy. **Command mode:** Route map
[no] set ip next-hop *<IP addresses>* **[access-list** *<1-32>***]** Sets the IP addresses for the next-hop to which packets are forwarded for each specified access list. When multiple addresses are specified they are prioritized in the order in which they are entered. Each next-hop must be an adjacent router. Use the **no** form of the command to remove the entry. **Command mode:** Route map
[no] set ip next-hop verify-availability *<IP address> <sequence (1-255)>* **[arp|icmp] [interval** *<1-60>***] [retry** *<1-3>***] [access-list** *<1-32>***]** Performs health-checking on and inserts the next hop IP address at the specified place (*sequence*) in the specified access list using ARP or ICMP as the tracking protocol. If not successful, the command will retry the health check at regular intervals of the specified number of seconds for the number of retries specified by `retry`. Use the **no** form of the command to remove the entry. Default values are `arp`, `2` seconds, and `3` retries. **Note:** This command overrides the "**set ip next-hop** *<IP address>*" command. **Command mode:** Route map
[no] set ip precedence *<precedence value>* **[access-list** *<1-32>***]** Sets the IP precedence value in the IP header for packets that match route map policy. You can choose a precendence value between 0 and 7 or one of the following: o `routine` sets routine precedence o `priority` sets priority precedence (1) o `immediate` sets immediate precedence (2) o `flash` sets flash precedence (3) o `flash-overrride` sets flash override precedence (4) o `critical` sets critical precedence (5) o `internet` sets internetwork control precedence (6) o `network` sets network precedence (7) **Command mode:** Route map

Table 273. *IP Next Hop Configuration Options*

Command Syntax and Usage
[no] ip policy route-map *<1-255>* Applies the route map to an IP interface that has a VLAN configured. **Command mode:** Interface IP
show route-map *<1-255>* Displays the current route map configuration. **Command mode:** All
show route-map *<1-255>* **access-list** *<1-32>* Displays the current Access List configuration. **Command mode:** All
show ip policy Displays the current routing policy information. **Command mode:** All
show ip policy statistics Displays statistics for the current routing policy. **Command mode:** All

Autonomous System Filter Path Configuration

Note: The *path number* represents the AS path you wish to configure.

Table 274. *AS Filter Configuration Options*

Command Syntax and Usage
as-path-list *<1-8>* **action {permit|deny}** Permits or denies Autonomous System filter action. **Command mode:** Route map
as-path-list *<1-8>* **as-path** *<1-65535>* Sets the Autonomous System filter's path number. **Command mode:** Route map
[no] as-path-list *<1-8>* **enable** Enables or disables the Autonomous System filter. **Command mode:** Route map
no as-path-list *<1-8>* Deletes the Autonomous System filter. **Command mode:** Route map
show route-map *<1-255>* **as-path-list** *<1-8>* Displays the current Autonomous System filter configuration. **Command mode:** All

Routing Information Protocol Configuration

RIP commands are used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 275. *Routing Information Protocol Options*

Command Syntax and Usage
`router rip` Enter Router RIP configuration mode. **Command mode:** Global configuration
`[no] enable` Globally enables or disables RIP. **Command mode:** Router RIP
`[no] redistribute {ebgp|eospf|fixed|ibgp|ospf|static}` Configures RIP route distribution. To view command options, see page 537. **Command mode:** Router RIP
`timers update` *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is `30` seconds. **Command mode:** Router RIP
`show ip rip` Displays the current RIP configuration. **Command mode:** All

RIP Interface Configuration

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

Note: Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 276. *RIP Interface Options*

Command Syntax and Usage
ip rip authentication key *<password>* Configures the authentication key password. **Command mode:** Interface IP
no ip rip authentication key Removes the authentication key password. **Command mode:** Interface IP
ip rip authentication type password *<password>* Configures the authentication type. The default is none. **Command mode:** Interface IP
no ip rip authentication type Removes the authentication type. **Command mode:** Interface IP
ip rip default-action {listen|supply|both} When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. The default value is none. **Command mode:** Interface IP
no ip rip default-action Configures the switch to reject RIP default routes. **Command mode:** Interface IP
[no] ip rip enable Enables or disables RIP on the current interface. **Command mode:** Interface IP
[no] ip rip listen When enabled, the switch learns routes from other routers. The default value is enabled. **Command mode:** Interface IP

Table 276. *RIP Interface Options (continued)*

Command Syntax and Usage
ip rip metric *<1-15>* Configures the route metric, which indicates the relative distance to the destination. The default value is 1. **Command mode:** Interface IP
[no] ip rip multicast-updates Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is enabled. **Command mode:** Interface IP
[no] ip rip poison When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is disabled. **Command mode:** Interface IP
[no] ip rip split-horizon Enables or disables split horizon. The default value is enabled. **Command mode:** Interface IP
[no] ip rip supply When enabled, the switch supplies routes to other routers. The default value is enabled. **Command mode:** Interface IP
[no] ip rip triggered Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is enabled. **Command mode:** Interface IP
ip rip version {1|2|both} Configures the RIP version used by this IP interface. The default value is version 2. **Command mode:** Interface IP
show interface ip *<1-128>* **rip** Displays the current settings for the RIP interface. **Command mode:** All

RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 277. *RIP Redistribution Options*

Command Syntax and Usage
[no] redistribute {fixed|static|ospf|eospf|ebgp|ibgp} {<*1-255*>**|all}** Adds or removes selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma(,). To add or remove all 255 route maps, type `all`. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed. **Command mode:** Router RIP
redistribute {fixed|static|ospf|eospf|ebgp|ibgp} export *<metric number (1-15)>* Exports the routes of this protocol in which the metric and metric type are specified. **Command mode:** Router RIP
no redistribute {fixed|static|ospf|eospf|ebgp|ibgp} export Stops exporting the routes of the specified protocol. **Command mode:** Router RIP
show ip rip redistribute Displays the current RIP route redistribute configuration. **Command mode:** All

Open Shortest Path First Configuration

The following table describes the OSPF commands.

Table 278. *OSPF Configuration Options*

Command Syntax and Usage
router ospf Enter Router OSPF configuration mode. **Command mode:** Global configuration
area *<0-19>* Configures OSPF area index. See page 539 to view command options. **Command mode:** Router OSPF
area-range *<1-16>* Configures summary routes for up to 16 IP addresses. See page 541 to view command options. **Command mode:** Router OSPF
area-virtual-link *<1-3>* Configures the Virtual Links used to configure OSPF for a Virtual Link. See page 544 to view command options. **Command mode:** Router OSPF
default-information *<1-16777214> <AS external metric type (1-2)>* Sets one default route among multiple choices in an area. **Command mode:** Router OSPF
no default-information Removes the default route information. **Command mode:** Router OSPF
[no] enable Enables or disables OSPF on the G8272. **Command mode:** Router OSPF
host *<1-128>* Configures OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 546 to view command options. **Command mode:** Router OSPF
lsdb-limit *<LSDB limit (0-16384, 0 for no limit)>* Sets the link state database limit. **Command mode:** Router OSPF

Table 278. *OSPF Configuration Options (continued)*

Command Syntax and Usage
message-digest-key *<key ID (1-255)>* **md5-key** *<text string>* Assigns a string to MD5 authentication key. **Command mode:** Router OSPF
no message-digest-key *<key ID (1-255)>* Removes the MD5 authentication key. **Command mode:** Router OSPF
redistribute {fixed|static|rip|ebgp|ibgp} Configures OSPF route redistribution. See page 547 to view command options. **Command mode:** Router OSPF
show ip ospf Displays the current OSPF configuration settings. **Command mode:** All

Area Index Configuration

The following table describes the Area Index commands.

Table 279. *Area Index Configuration Options*

Command Syntax and Usage
area *<0-19>* **area-id** *<IP address>* Defines the IP address of the OSPF area number. **Command mode:** Router OSPF
area *<0-19>* **authentication-type {password|md5}** Sets the authentication type. o `password` authenticates simple passwords so that only trusted routing devices can participate. o `md5` is used when MD5 cryptographic authentication is required. **Command mode:** Router OSPF
no area *<0-19>* **authentication-type** Removes the authentification type. **Command mode:** Router OSPF
[no] area *<0-19>* **enable** Enables or disables the OSPF area. **Command mode:** Router OSPF

Table 279. *Area Index Configuration Options (continued)*

Command Syntax and Usage
area *<0-19>* **spf-interval** *<1-255>* Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm. The default value is **10** seconds. **Command mode:** Router OSPF
area *<0-19>* **stub-metric** *<1-65535>* Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions. Metric value assigns the priority for choosing the switch for default route. **Command mode:** Router OSPF
area *<0-19>* **type {transit|stub|nssa}** Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. o **transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. o **stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. o **nssa:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. **Command mode:** Router OSPF
no area *<0-19>* Deletes the OSPF area. **Command mode:** Router OSPF
show ip ospf area *<0-19>* Displays the current OSPF configuration. **Command mode:** All

OSPF Summary Range Configuration

The following table describes the OSPF Summary Range commands.

Table 280. *OSPF Summary Range Configuration Options*

Command Syntax and Usage
area-range *<1-16>* **address** *<IP address>* **[***<IP netmask>***]** Displays the base IP address or the IP address mask for the range. **Command mode:** Router OSPF
area-range *<1-16>* **area** *<0-19>* Displays the area index used by the G8272. **Command mode:** Router OSPF
[no] area-range *<1-16>* **enable** Enables or disables the OSPF summary range. **Command mode:** Router OSPF
[no] area-range *<1-16>* **hide** Hides or shows the OSPF summary range. **Command mode:** Router OSPF
no area-range *<1-16>* Deletes the OSPF summary range. **Command mode:** Router OSPF
show ip ospf area-range *<1-16>* Displays the current OSPF summary range. **Command mode:** All

OSPF Interface Configuration

The following table describes the OSPF Interface commands.

Table 281. *OSPF Interface Configuration Options*

Command Syntax and Usage
ip ospf area *<0-19>* Configures the OSPF area index. **Command mode:** Interface IP
ip ospf cost *<1-65535>* Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. **Command mode:** Interface IP
ip ospf dead-interval *<1-65535>* **ip ospf dead-interval** *<1000-65535 ms>* Configures the health parameters of a `hello` packet, in seconds or milliseconds, before declaring a silent router to be down. **Command mode:** Interface IP
[no] ip ospf enable Enables or disables the OSPF interface. **Command mode:** Interface IP
ip ospf hello-interval *<1-65535>* **ip ospf hello-interval** *<50-65535 ms>* Configures the interval, in seconds or milliseconds, between the `hello` packets for the interfaces. **Command mode:** Interface IP
ip ospf key *<key string>* Sets the authentication key to clear the password. **Command mode:** Interface IP
no ip ospf key Removes the authentification key to clear the password. **Command mode:** Interface IP
ip ospf message-digest-key *<1-255>* Assigns an MD5 key to the interface. **Command mode:** Interface IP
no ip ospf message-digest-key Removes the MD5 key form the interface. **Command mode:** Interface IP

Table 281. *OSPF Interface Configuration Options (continued)*

Command Syntax and Usage
[no] ip ospf passive-interface Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established. **Command mode:** Interface IP
[no] ip ospf point-to-point Sets the interface as point-to-point. **Command mode:** Interface IP
ip ospf priority *<0-255>* Configures the priority value for the G8272's OSPF interfaces. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR). **Command mode:** Interface IP
ip ospf retransmit-interval *<1-3600>* Configures the retransmit interval in seconds. **Command mode:** Interface IP
ip ospf transit-delay *<1-3600>* Configures the transit delay in seconds. **Command mode:** Interface IP
no ip ospf Deletes the OSPF interface. **Command mode:** Interface IP
show interface ip *<1-128>* **ospf** Displays the current settings for OSPF interface. **Command mode:** All

OSPF Virtual Link Configuration

The following table describes the OSPF Virtual Link commands.

Table 282. *OSPF Virtual Link Configuration Options*

Command Syntax and Usage
area-virtual-link *<1-3>* **area** *<0-19>* Configures the OSPF area index for the virtual link. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **dead-interval** *<1-65535>* **area-virtual-link** *<1-3>* **dead-interval** *<1000-65535 ms>* Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is `40` seconds. **Command mode:** Router OSPF
[no] area-virtual-link *<1-3>* **enable** Enables or disables OSPF virtual link. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **hello-interval** *<1-65535>* **area-virtual-link** *<1-3>* **hello-interval** *<50-65535 ms>* Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is `10` seconds. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **key** *<password>* Configures the password (up to eight characters) for each virtual link. The default setting is `none`. **Command mode:** Router OSPF
no area-virtual-link *<1-3>* **key** Removes the authentification key. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **message-digest-key** *<1-255>* Sets MD5 key ID for each virtual link. The default setting is `none`. **Command mode:** Router OSPF
no area-virtual-link *<1-3>* **message-digest-key** Removes the MD5 key ID for the specified virtual link. **Command mode:** Router OSPF

Table 282. *OSPF Virtual Link Configuration Options (continued)*

Command Syntax and Usage
area-virtual-link *<1-3>* **neighbor-router** *<IP address>* Configures the router ID of the virtual neighbor. The default value is `0.0.0.0`. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **retransmit-interval** *<1-3600>* Configures the retransmit interval, in seconds. The default value is `5` seconds. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **transit-delay** *<1-3600>* Configures the delay in transit, in seconds. The default value is `1` second. **Command mode:** Router OSPF
no area-virtual-link *<1-3>* Deletes OSPF virtual link. **Command mode:** Router OSPF
show ip ospf area-virtual-link *<1-3>* Displays the current OSPF virtual link settings. **Command mode:** All

OSPF Host Entry Configuration

The following table describes the OSPF Host Entry commands.

Table 283. *OSPF Host Entry Configuration Options*

Command Syntax and Usage
host *<1-128>* **address** *<IP address>* Configures the base IP address for the host entry. **Command mode:** Router OSPF
host *<1-128>* **area** *<0-19>* Configures the area index of the host. **Command mode:** Router OSPF
host *<1-128>* **cost** *<1-65535>* Configures the cost value of the host. **Command mode:** Router OSPF
[no] host *<1-128>* **enable** Enables or disables the OSPF host entry. **Command mode:** Router OSPF
no host *<1-128>* Deletes OSPF host entry. **Command mode:** Router OSPF
show ip ospf host *<1-128>* Displays the current OSPF host entries. **Command mode:** All

OSPF Route Redistribution Configuration

The following table describes the OSPF Route Redistribution commands.

Table 284. *OSPF Route Redistribution Configuration Options*

Command Syntax and Usage
[no] redistribute {fixed|static|rip|ebgp|ibgp} *<1-255>* Adds or removes selected routing map to the rmap list. This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed. **Command mode:** Router OSPF
redistribute {fixed|static|rip|ebgp|ibgp} export *<metric (1-16777214)> <AS external metric type (1-2)>* Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. **Command mode:** Router OSPF
no redistribute {fixed|static|rip|ebgp|ibgp} export Stops exporting the routes of the protocol. **Command mode:** Router OSPF
show ip ospf redistribute Displays the current route map settings. **Command mode:** All

OSPF MD5 Key Configuration

The following table describes the OSPF MD5 Key commands.

Table 285. *OSPF MD5 Key Options*

Command Syntax and Usage
message-digest-key *<1-255>* **md5-key** *<1-16 characters>* Sets the authentication key for this OSPF packet. **Command mode:** Router OSPF
no message-digest-key *<1-255>* Deletes the authentication key for this OSPF packet. **Command mode:** Router OSPF
show ip ospf message-digest-key *<1-255>* Displays the current MD5 key configuration. **Command mode:** All

Open Shortest Path First Version 3 Configuration

The following table describes the OSPFv3 commands.

Table 286. *OSPFv3 Configuration Options*

Command Syntax and Usage
`[no] ipv6 router ospf` Enter OSPFv3 configuration mode. **Command mode**: Global configuration
`abr-type [standard|cisco|ibm]` Configures the Area Border Router (ABR) type, as follows: o Standard o Cisco o IBM The default setting is `standard`. **Command mode**: Router OSPF3
`no abr-type` Resets the Area Border Router (ABR) type to its default value - `standard`. **Command mode:** Router OSPF3
`as-external lsdb-limit` *<LSDB limit (0-2147483647, -1 for no limit)>* Sets the link state database limit. The default value is `-1`. **Command mode**: Router OSPF3
`[no] enable` Enables or disables OSPFv3 on the switch. **Command mode**: Router OSPF3
`exit-overflow-interval` *<0-4294967295>* Configures the number of seconds that a router takes to exit Overflow State. The default value is `0`. **Command mode**: Router OSPF3

Table 286. *OSPFv3 Configuration Options (continued)*

Command Syntax and Usage
neighbor *<1-256>* **{address** *<IPv6 address>***|interface** *<1-126>***| |priority** *<0-255>***}** Configures directly reachable routers over non-broadcast networks.This is required for non-broadcast multiple access (NBMA) networks and optional for Point-to-Multipoint networks. o `address` configures the neighbor's IPv6 address. o `interface` configures the OSPFv3 interface used for the neighbor entry. o `priority` configures the priority value used for the neighbor entry. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the neighbor cannot be used as Designated Router or Backup Designated Router. The default value is `1`. **Command mode**: Router OSPF3
[no] neighbor *<1-256>* **enable** Enables or disables the specified neighbor. **Command mode:** Router OSPF3
no neighbor *<1-256>* Deletes the neighbor entry. **Command mode**: Router OSPF3
[no] nssaAsbrDfRtTrans Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is `disabled`. **Command mode**: Router OSPF3
reference-bandwidth *<0-4294967295>* Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is `100,000`. **Command mode**: Router OSPF3
router-id *<IPv4 address>* Defines the router ID. **Command mode**: Router OSPF3

Table 286. *OSPFv3 Configuration Options (continued)*

Command Syntax and Usage
timers spf *<SPF delay (0-65535)> <SPF hold time (0-65535)>* Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5 seconds. Configures the number of seconds between SPF calculations. The default value is 10 seconds. **Command mode**: Router OSPF3
no timers spf Resets the SPF timers to their default values - SPF delay to 5 seconds and SPF hold time to 10 seconds. **Command mode:** Router OSPF3
show ipv6 ospf Displays the current OSPF configuration settings. **Command mode**: All

OSPFv3 Area Index Configuration

The following table describes the OSPFv3 Area Index commands.

Table 287. *OSPFv3 Area Index Configuration Options*

Command Syntax and Usage
area *<0-2>* **area-id** *<IP address>* Defines the IP address of the OSPFv3 area number. **Command mode**: Router OSPF3
area *<0-2>* **default-metric** *<metric value (1-16777215)>* Configures the cost for the default summary route in a stub area or NSSA. **Command mode**: Router OSPF3
area *<0-2>* **default-metric type** *<1-3>* Configures the default metric type applied to the route. **Note:** This command applies only to area type of Stub/NSSA. **Command mode**: Router OSPF3
no area *<0-2>* **default-metric** Resets the cost for the default summary route to its default value of 1. **Command mode:** Router OSPF3
[no] area *<0-2>* **enable** Enables or disables the OSPF area. **Command mode**: Router OSPF3

Table 287. *OSPFv3 Area Index Configuration Options (continued)*

Command Syntax and Usage
area *<0-2>* **stability-interval** *<1-255>* Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is `40` seconds. **Command mode**: Router OSPF3
no area *<0-2>* **stability-interval** Resets the stability interval for the NSSA to its default value of `40` seconds. **Command mode:** Router OSPF3
area *<0-2>* **translation-role {always|candidate}** Configures the translation role for an NSSA area, as follows: o `always`: Type 7 LSAs are always translated into Type 5 LSAs. o `candidate`: An NSSA border router participates in the translator election process. The default setting is `candidate`. **Command mode**: Router OSPF3
no area *<0-2>* **translation-role** Resets the translation role for the NSSA to its default value - `candidate`. **Command mode:** Router OSPF3
area *<0-2>* **type {transit|stub|nssa} [no-summary]** Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. o `transit` allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. o `stub` is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. o `nssa` (Not-So-Stubby Area) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas. `no-summary` enables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA. The default setting is `disabled`. **Command mode**: Router OSPF3

Table 287. *OSPFv3 Area Index Configuration Options (continued)*

Command Syntax and Usage
no area *<0-2>* Deletes the OSPF area. **Command mode**: Router OSPF3
show ipv6 ospf {areas|area *<0-2>***}** Displays the current OSPFv3 area configuration. **Command mode**: All

OSPFv3 Summary Range Configuration

The following table describes the OSPFv3 Summary Range commands.

Table 288. *OSPFv3 Summary Range Configuration Options*

Command Syntax and Usage
area-range *<1-16>* **address** *<IPv6 address> <prefix length (1-128)>* Configures the base IPv6 address and subnet prefix length for the range. **Command mode**: Router OSPF3
area-range *<1-16>* **area** *<area index (0-2)>* Configures the area index used by the switch. **Command mode**: Router OSPF3
[no] area-range *<1-16>* **enable** Enables or disables the OSPFv3 summary range. **Command mode**: Router OSPF3
[no] area-range *<1-16>* **hide** Hides or shows the OSPFv3 summary range. **Command mode**: Router OSPF3
area-range *<1-16>* **lsa-type {summary|Type7}** Configures the LSA type, as follows: o Summary LSA o Type7 LSA **Command mode**: Router OSPF3
area-range *<1-16>* **tag** *<0-4294967295>* Configures the route tag. **Command mode**: Router OSPF3
no area-range *<1-16>* Deletes the OSPFv3 summary range. **Command mode**: Router OSPF3
show ipv6 ospf area-range Displays the current OSPFv3 summary range. **Command mode**: All

OSPFv3 AS-External Range Configuration

The following table describes the OSPFv3 AS-External Range commands.

Table 289. *OSPFv3 AS_External Range Configuration Options*

Command Syntax and Usage
summary-prefix *<1-16>* **address** *<IPv6 address> <IPv6 prefix length (1-128)>* Configures the base IPv6 address and the subnet prefix length for the range. **Command mode**: Router OSPF3
summary-prefix *<1-16>* **aggregation-effect {allowAll|denyAll| |advertise|not-advertise}** Configures the aggregation effect, as follows: o `allowAll`: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range. o `denyAll`: Type-5 and Type-7 LSAs are not generated. o `advertise`: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area. o `not-advertise`: If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area. **Command mode**: Router OSPF3
summary-prefix *<1-16>* **area** *<area index (0-2)>* Configures the area index used by the switch. **Command mode**: Router OSPF3
[no] summary-prefix *<1-16>* **translation** When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is `disabled`. **Command mode**: Router OSPF3
[no] summary-prefix *<1-16>* **enable** Enables or disables the OSPFv3 AS-external range. **Command mode**: Router OSPF3
no summary-prefix *<1-16>* Deletes the OSPFv3 AS-external range. **Command mode**: Router OSPF3
show ipv6 ospf summary-prefix *<1-16>* Displays the current OSPFv3 AS-external range. **Command mode**: All

OSPFv3 Interface Configuration

The following table describes the OSPFv3 Interface commands.

Table 290. *OSPFv3 Interface Configuration Options*

Command Syntax and Usage
interface ip *<1-128>* Enter Interface IP mode, from Global Configuration mode. **Command mode**: Global configuration
ipv6 ospf area *<0-2>* Configures the OSPFv3 area index. **Command mode**: Interface IP
ipv6 ospf area *<0-2>* **instance** *<0-255>* Configures the instance ID for the interface. **Command mode**: Interface IP
ipv6 ospf cost *<1-65535>* Configures the metric value for sending a packet on the interface. **Command mode**: Interface IP
no ipv6 ospf cost Removes the metric value for sending a packet on the interface. **Command mode:** Interface IP
ipv6 ospf dead-interval *<1-65535>* Configures the time period, in seconds, for which the router waits for `hello` packet from the neighbor before declaring this neighbor down. **Command mode**: Interface IP
no ipv6 ospf dead-interval Resets the dead interval for hello packets to its default value. **Command mode:** Interface IP
[no] ipv6 ospf enable Enables or disables OSPFv3 on the interface. **Command mode**: Interface IP
ipv6 ospf hello-interval *<1-65535>* Configures the indicated interval, in seconds, between the `hello` packets, that the router sends on the interface. **Command mode**: Interface IP
no ipv6 ospf hello-interval Resets the hello interval for hello packets to its default value. **Command mode:** Interface IP

Table 290. *OSPFv3 Interface Configuration Options (continued)*

Command Syntax and Usage
[no] ipv6 ospf linklsasuppress Enables or disables Link LSA suppression. When suppressed, no Link LSAs are originated. The default setting is `disabled`. **Command mode**: Interface IP
ipv6 ospf network {broadcast|non-broadcast| |point-to-multipoint|point-to-point} Configures the network type for the OSPFv3 interface: o `broadcast`: network where all routers use the broadcast capability o `non-broadcast`: non-broadcast multiple access (NBMA) network supporting pseudo-broadcast (multicast and broadcast traffic is configured manually) o `point-to-multipoint`: network where multiple point-to-point links are set up on the same interface o `point-to-point`: network that joins a single pair of routers The default value is `broadcast`. **Command mode**: Interface IP
[no] ipv6 ospf passive-interface Enables or disables the `passive` setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed. **Command mode**: Interface IP
ipv6 ospf poll-interval *<0-4294967295>* Configures the poll interval in seconds for neighbors in NBMA networks. The default value is `120` seconds. **Command mode**: Interface IP
no ipv6 ospf poll-interval Configures the poll interval in seconds for neighbors in NBMA and point-to-multipoint networks to its default `120` seconds value. **Command mode**: Interface IP
ipv6 ospf priority *<priority value (0-255)>* Configures the priority value for the switch's OSPFv3 interface. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR). **Command mode**: Interface IP
no ipv6 ospf priority Resets the priority value for the switch's OSPFv3 interface to its default value. **Command mode:** Interface IP

Table 290. *OSPFv3 Interface Configuration Options (continued)*

Command Syntax and Usage
ipv6 ospf retransmit-interval *<1-1800>* Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface. **Command mode**: Interface IP
no ipv6 ospf retransmit-interval Resets the interval between LSA retransmissions for adjacencies belonging to the current interface to its default value. **Command mode:** Interface IP
ipv6 ospf transmit-delay *<1-1800>* Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. **Command mode**: Interface IP
no ipv6 ospf transmit-delay Resets the estimated time taken to transmit LS update packet over the current interface to its default value. **Command mode:** Interface IP
no ipv6 ospf Deletes OSPFv3 from interface. **Command mode**: Interface IP
show ipv6 ospf interface Displays the current settings for OSPFv3 interface. **Command mode**: All

OSPFv3 over IPSec Configuration

The following table describes the OSPFv3 over IPsec Configuration commands.

Table 291. *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
ipv6 ospf authentication ipsec enable Enables IPsec. **Command mode:** Interface IP
ipv6 ospf authentication ipsec spi *<256-4294967295>* **{md5|sha1}** *<authentication key (hexadecimal)>* Configures the Security Parameters Index (SPI), algorithm, and authentication key for the Authentication Header (AH). The algorithms supported are: o MD5 (hexadecimal key length is 32) o SHA1 (hexadecimal key length is 40) **Command mode:** Interface IP
no ipv6 ospf authentication ipsec spi *<256-4294967295>* Disables the specified Authentication Header (AH) SPI. **Command mode:** Interface IP
ipv6 ospf authentication ipsec default Resets the Authentication Header (AH) configuration to default values. **Command mode:** Interface IP
ipv6 ospf encryption ipsec enable Enables OSPFv3 encryption for this interface. **Command mode:** Interface IP

Table 291. *Layer 3 IPsec Configuration Options (continued)*

Command Syntax and Usage
ipv6 ospf encryption ipsec spi *<256-4294967295>* **esp {3des|aes-cbc|null}** *<encryption key (hexadecimal)>* **{md5|sha1|none}** *<authentication key (hexadecimal)>* Configures the Security Parameters Index (SPI), encryption algorithm, authentication algorithm, and authentication key for the Encapsulating Security Payload (ESP). The ESP algorithms supported are: o `3des` (hexadecimal key length is 48) o `aes-cbc` (hexadecimal key length is 32) o `null` means ESP with no encryption. The authentication algorithms supported are: o `md5` (hexadecimal key length is 32) o `sha1` (hexadecimal key length is 40) o `none` means ESP with no authentication. **Note:** If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. If an encryption algorithm is specified (3DES or AES-CBC), the authentication algorithm can be `none`. **Command mode:** Interface IP
no ipv6 ospf encryption ipsec spi *<256-4294967295>* Disables the specified Encapsulating Security Payload (ESP) SPI. **Command mode:** Interface IP
ipv6 ospf encryption ipsec default Resets the Encapsulating Security Payload (ESP) configuration to default values. **Command mode:** Interface IP

OSPFv3 Virtual Link Configuration

The following table describes the OSPFv3 Virtual Link commands.

Table 292. *OSPFv3 Virtual Link Configuration Options*

Command Syntax and Usage
area-virtual-link *<1-3>* **area** *<0-2>* Configures the OSPF area index. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **dead-interval** *<1-65535>* Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down. **Command mode**: Router OSPF3
[no] area-virtual-link *<1-3>* **enable** Enables or disables OSPF virtual link. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **hello-interval** *<1-65535)>* Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **neighbor-router** *<NBR router ID (IP address)>* Configures the router ID of the virtual neighbor. The default setting is `0.0.0.0`. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **retransmit-interval** *<1-3600>* Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is `5` seconds. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **transmit-delay** *<1-3600>* Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. **Command mode**: Router OSPF3
no area-virtual-link *<1-3>* Deletes OSPF virtual link. **Command mode**: Router OSPF3
show ipv6 ospf area-virtual-link Displays the current OSPFv3 virtual link settings. **Command mode**: All

OSPFv3 over IPSec for Virtual Link Configuration

The following table describes the OSPFv3 over IPsec for Virtual Link Configuration commands.

Table 293. *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
area-virtual-link *<1-3>* **authentication ipsec enable** Enables OSPFv3 IPsec authentication . **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **authentication ipsec spi** *<256-4294967295>* **{md5** *<md5 key>***|sha1** *<sha1 key>***}** Configures the OSPFv3 security parameter index authentication. **Command mode:** Router OSPF3
no area-virtual-link *<1-3>* **authentication ipsec spi** *<256-4294967295>* Removes the specified OSPFv3 Security Parameters Index (SPI). **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **authentication ipsec default** Resets the IPsec Authentication Header (AH) to its default values. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **encryption ipsec enable** Enables OSPFv3 IPsec encryption. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **encryption ipsec spi** *<256-4294967295>* **esp {3des|aes-cbc|null}** *<encryption key (hexadecimal)>* **{md5|sha1|none}** *<authentication key (hexadecimal)>* Configures the Security Parameters Index (SPI), encryption algorithm, authentication algorithm, and authentication key for the Encapsulating Security Payload (ESP). The ESP algorithms supported are: o `3des` (hexadecimal key length is 48) o `aes-cbc` (hexadecimal key length is 32) o `null` means ESP with no encryption. The authentication algorithms supported are: o `md5` (hexadecimal key length is 32) o `sha1` (hexadecimal key length is 40) o `none` means ESP with no authentication. **Note:** If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. If an encryption algorithm is specified (3DES or AES-CBC), the authentication algorithm can be `none`. **Command mode:** Router OSPF3

Table 293. *Layer 3 IPsec Configuration Options (continued)*

Command Syntax and Usage
no area-virtual-link *<1-3>* **encryption ipsec spi** *<256-4294967295>* Disables the specified Encapsulating Security Payload (ESP) SPI. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **encryption ipsec default** Resets the IPsec encryption configuration to its default values. **Command mode:** Router OSPF3
show ipv6 ospf area-virtual-link Displays the current OSPFv3 virtual link settings. **Command mode**: All

OSPFv3 Host Entry Configuration

The following table describes the OSPFv3 Host Entry commands.

Table 294. *OSPFv3 Host Entry Configuration Options*

Command Syntax and Usage
host *<1-128>* **address** *<IPv6 address> <prefix length (1-128)>* Configures the base IPv6 address and the subnet prefix length for the host entry. **Command mode**: Router OSPF3
host *<1-128>* **area** *<0-2>* Configures the area index of the host. **Command mode**: Router OSPF3
host *<1-128>* **cost** *<1-65535>* Configures the cost value of the host. **Command mode**: Router OSPF3
[no] host *<1-128>* **enable** Enables or disables the host entry. **Command mode**: Router OSPF3
no host *<1-128>* Deletes the host entry. **Command mode**: Router OSPF3
show ipv6 ospf host [*<1-128>***]** Displays the current OSPFv3 host entries. **Command mode**: All

OSPFv3 Redistribute Entry Configuration

The following table describes the OSPFv3 Redistribute Entry commands.

Table 295. *OSPFv3 Redist Entry Configuration Options*

Command Syntax and Usage
redist-config *<1-128>* **address** *<IPv6 address>* *<IPv6 prefix length (1-128)>* Configures the base IPv6 address and the subnet prefix length for the redistribution entry. **Command mode**: Router OSPF3
[no] redist-config *<1-128>* **enable** Enables or disables the OSPFv3 redistribution entry. **Command mode**: Router OSPF3
redist-config *<1-128>* **metric-type {asExttype1|asExttype2}** Configures the metric type applied to the route before it is advertised into the OSPFv3 domain. **Command mode**: Router OSPF3
redist-config *<1-128>* **metric-value** *<1-16777215>* Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain. **Command mode**: Router OSPF3
redist-config *<1-128>* **tag** *<0-4294967295>* Configures the route tag. **Command mode**: Router OSPF3
no redist-config *<1-128>* **tag** Removes the route tag. **Command mode:** Router OSPF3
no redist-config *<1-128>* Deletes the OSPFv3 redistribution entry. **Command mode**: Router OSPF3
show ipv6 ospf redist-config *<1-128>* Displays the current OSPFv3 redistribution configuration for the specified entry. **Command mode**: All

OSPFv3 Redistribute Configuration

The following table describes the OSPFv3 Redistribute commands.

Table 296. *OSPFv3 Redistribute Configuration Options*

Command Syntax and Usage
redistribute {connected|static} export *<metric value (1-16777215)> <metric type (1-2)>* **[***<tag (0-4294967295)>***]** Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. **Command mode**: Router OSPF3
no redistribute {connected|static} export Stops exporting the routes of the protocol. **Command mode:** Router OSPF3
show ipv6 ospf Displays the current OSPFv3 route redistribution settings. **Command mode**: All

Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the "best" route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current Enterprise NOS implementation, the RackSwitch G8272 does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

Note: Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 297. *Border Gateway Protocol Options*

Command Syntax and Usage
router bgp Enter Router BGP configuration mode. **Command mode:** Global configuration
aggregate-address *<1-16>* Configures aggregation IP address. To view command options, see page 570. **Command mode:** Router BGP
as *<0-65535>* Set Autonomous System number. **Command mode:** Router BGP
[no] asn4comp Enables or disables ASN4 to ASN2 compatibility. **Command mode:** Router BGP
[no] bestpath as-path multipath-relax Changes the default best path selection configuration by allowing load sharing across different AS-paths of equal length. **Command mode:** Router BGP
[no] client-to-client reflection Enables or disables client-to-client IBGP route reflection when operating as a route reflector. The default state is `enabled`. **Command mode:** Router BGP

Table 297. *Border Gateway Protocol Options (continued)*

Command Syntax and Usage
`cluster-id` *<IP address>* Specifies the router's Cluster ID used when operating as a route reflector. Route reflectors that are part of the same cluster (assigned to the same group of clients) must use identical Cluster IDs. **Command mode:** Router BGP
`no cluster-id` Removes the router's Cluster ID. **Command mode:** Router BGP
`dscp` *<0-63>* Set the DSCP marking value. **Command mode:** Router BGP
`[no] enable` Globally enables or disables BGP. **Command mode:** Router BGP
`local-preference` *<0-4294967294>* Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP. **Command mode:** Router BGP
`maximum-paths [ibgp]` *<1-32>* Set maximum paths allowed for an external route. `ibgp` will set the maximum paths allowed for an internal route. By default, BGP will install only one path to the IP routing table. **Command mode:** Router BGP
`no maximum-paths [ibgp]` Resets the maximum paths allowed for an external route to its default value of `1`. The `ibgp` option resets the maximum paths allowed for an internal route. **Command mode:** Router BGP
`neighbor {`*<peer number (1-96)>***`|group`** *<1-8>***`}`** Configures each BGP *peer.* Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view command options, see page 567. **Command mode:** Router BGP

Table 297. *Border Gateway Protocol Options (continued)*

Command Syntax and Usage
[no] set ip next-hop peer-address Applied on output, sets the next-hop of the advertised matching routes to the current peer address of the local router. Applied on input, sets the next-hop of the received matching routes to the neighbor address, overriding other existing next-hops. Use the no form of the command to remove the entry. **Command mode:** Route map
show ip bgp Displays the current BGP configuration. **Command mode:** All

BGP Peer Configuration

Use these commands to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

Table 298. *BGP Peer Configuration Options*

Command Syntax and Usage
neighbor *<1-96>* **advertisement-interval** *<1-65535>* Sets time, in seconds, between advertisements. The default value is 60 seconds. **Command mode:** Router BGP
[no] neighbor *<1-96>* **next-hop-self** Enables or disables enforcing the use the router's own IP address as next-hop attribute when sending BGP updates to the peer. **Note:** Applicable only for EBGP routes. **Command mode:** Router BGP
[no] neighbor *<1-96>* **passive** Enables or disables BGP passive mode, which prevents the switch from initiating BGP connections with peers. Instead, the switch waits for the peer to send an open message first. **Command mode:** Router BGP
neighbor *<1-96>* **password** *<1-16 characters>* Configures the BGP peer password. **Command mode:** Router BGP
no neighbor *<1-96>* **password** Removes the BGP peer password. **Command mode:** Router BGP

Table 298. *BGP Peer Configuration Options (continued)*

Command Syntax and Usage
neighbor *<1-96>* **redistribute** Configures BGP neighbor redistribution. To view command options, see page 571. **Command mode:** Router BGP
neighbor *<1-96>* **remote-address** *<IP address>* Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is `0.0.0.0`. **Command mode:** Router BGP
neighbor *<1-96>* **remote-as** *<1-65535>* Sets the remote autonomous system number for the specified peer. **Command mode:** Router BGP
neighbor *<1-96>* **retry-interval** *<1-65535>* Sets connection retry interval, in seconds. The default value is `120` seconds. **Command mode:** Router BGP
neighbor *<1-96>* **route-map {in|out}** *<1-255>* Adds route map into in-route or out-route map list. **Command mode:** Router BGP
no neighbor *<1-96>* **route-map {in|out} {***<1-255>***|all}** Removes all route maps or a specific route map from in-route or out-route map list. **Command mode:** Router BGP
neighbor *<1-96>* **route-origination-interval** *<1-65535>* Sets the minimum time between route originations, in seconds. The default value is `15` seconds. **Command mode:** Router BGP
[no] neighbor *<1-96>* **route-reflector-client** Enables or disables the peer as a route reflector client. Configuring route reflector clients, implicitly sets up the local router as a route reflector. **Command mode:** Router BGP
[no] neighbor *<1-96>* **send-community** Enables or disables sending a community attribute to a BGP neighbor. **Command mode:** Router BGP

Table 298. *BGP Peer Configuration Options (continued)*

Command Syntax and Usage
neighbor *<1-96>* **shutdown** Disables this peer configuration. **Command mode:** Router BGP
no neighbor *<1-96>* **shutdown** Enables this peer configuration. **Command mode:** Router BGP
neighbor *<1-96>* **time-to-live** *<1-255>* Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded. This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of "hops" the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at `1`. **Note:** The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value). **Command mode:** Router BGP
no neighbor *<1-96>* **time-to-live** Disables the TTL feature. **Command mode:** Router BGP
neighbor *<1-96>* **timers hold-time** *<0, 3-65535>* Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is `180` seconds. **Command mode:** Router BGP
neighbor *<1-96>* **timers keep-alive** *<0-21845>* Sets the keep-alive time for the specified peer, in seconds. The default value is `60` seconds. **Command mode:** Router BGP
neighbor *<1-96>* **ttl-security hops** *<1-254>* Sets the minimum number of time-to-live (TTL) router hops an IP packet must have to not be discarded. **Command mode:** Router BGP

Table 298. *BGP Peer Configuration Options (continued)*

Command Syntax and Usage
no neighbor *<1-96>* **ttl-security hops** Disables the TTL security feature. **Command mode:** Router BGP
neighbor *<1-96>* **update-source {***<interface number (1-126)>***|** **|loopback** *<1-5>***}** Sets the source interface number for this peer. **Command mode:** Router BGP
no neighbor *<1-96>* Deletes this peer configuration. **Command mode:** Router BGP
show ip bgp neighbor [*<1-192>***]** Displays the current BGP peer configuration. **Command mode:** All

BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, in order to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 299. *BGP Aggregation Configuration Options*

Command Syntax and Usage
aggregate-address *<1-16> <IP address> <IP netmask>* Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is `0.0.0.0`. **Command mode:** Router BGP
[no] aggregate-address *<1-16>* **enable** Enables or disables this BGP aggregation. **Command mode:** Router BGP
no aggregate-address *<1-16>* Deletes this BGP aggregation. **Command mode:** Router BGP
show ip bgp aggregate-address [*<1-16>***]** Displays the current BGP aggregation configuration. **Command mode:** All

BGP Neighbor Redistribution Configuration

This menu enables you to redistribute routes learned from various routing information sources into BGP.

Table 300. *BGP Neighbor Redistribution Configuration Options*

Command Syntax and Usage
neighbor *<1-96>* **redistribute default-action {import| |originate|redistribute}** Sets default route action. Defaults routes can be configured as follows: o `import`: Import these routes. o `originate`: The switch sends a default route to peers if it does not have any default routes in its routing table. o `redistribute`: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol. **Command mode:** Router BGP
no neighbor *<1-96>* **redistribute default-action** Disables the default route action configuration. **Command mode:** Router BGP
neighbor *<1-96>* **redistribute default-metric** *<1-4294967294>* Sets default metric of advertised routes. **Command mode:** Router BGP
no neighbor *<1-96>* **redistribute default-metric** Disables the default metric configuration of advertised routes. **Command mode:** Router BGP
[no] neighbor *<1-96>* **redistribute {fixed|ospf|rip|static}** Enables or disables advertising fixed, OSPF, RIP or static routes. **Command mode:** Router BGP
show ip bgp neighbor *<1-192>* **redistribute** Displays current redistribution configuration. **Command mode:** All

BGP Peering Group Configuration

These commands enable you to configure BGP peering for a group of remote neighbors defined by a range of IP addresses. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group and a TCP session is established for an IP address in that subnet range, a new BGP neighbor is dynamically created as a member of that group and inherits the configuration from the peer group.

Table 301. *BGP Peering Group Configuration Options*

Command Syntax and Usage
neighbor group *<1-8>* **advertisement-interval** *<minimum advertisement time (1-65535)>* Sets time, in seconds, between advertisements. The default value is `60` seconds. **Command mode:** Router BGP
neighbor group *<1-8>* **listen limit** *<group limit (1-96)>* Sets the maximum number of BGP dynamic peers. **Command mode:** Router BGP
neighbor group *<1-8>* **listen range** *<IPv4 address> <IPv4 subnet mask>* Defines the range of IP addresses that will be accepted for the group. **Command mode:** Router BGP
neighbor group *<1-8>* **name** *<1-32 characters>* Sets the name for the group. **Command mode:** Router BGP
no neighbor group *<1-8>* **name** Deletes the name for the group. **Command mode:** Router BGP
[no] neighbor group *<1-8>* **next-hop-self** Enables or disables enforcing the use the router's own IP address as next-hop attribute when sending BGP updates to the peering group. Applicable only for EBGP routes. **Command mode:** Router BGP
neighbor group *<1-8>* **password** *<1-16 characters>* Configures the BGP peer group password. **Command mode:** Router BGP
no neighbor group *<1-8>* **password** Deletes the BGP peer group password. **Command mode:** Router BGP

Table 301. *BGP Peering Group Configuration Options (continued)*

Command Syntax and Usage
neighbor group *<1-8>* **redistribute** Configures BGP neighbor group redistribution. To view command options, see page 576. **Command mode:** Router BGP
neighbor group *<1-8>* **remote-as** *<AS number (1-65535)>* **[alternate-as** *<AS number (1-65535)>***]** Adds a remote access server (RAS) into the RAS list. Using the `alternate-as` option you can add up to 5 alternate access servers. **Command mode:** Router BGP
neighbor group *<1-8>* **route-map {in|out}** *<route map ID (1-255)>* Adds route map into in-route or out-route map list. **Command mode:** Router BGP
no neighbor group *<1-8>* **route-map {in|out}** **{***<route map ID (1-255)>***|all}** Removes route map from in-route map list. **Command mode:** Router BGP
neighbor group *<1-8>* **route-origination-interval** *<min orig time (1-65535)>* Sets the minimum time between route originations, in seconds. The default value is `15` seconds. **Command mode:** Router BGP
[no] neighbor group *<1-8>* **route-reflector-client** Enables or disables the group as a route reflector client. Configuring route reflector clients, implicitly sets up the local router as a route reflector. **Command mode:** Router BGP
[no] neighbor group *<1-8>* **send-community** Enables or disables sending a community attribute to a BGP neighbor group. **Command mode:** Router BGP
no neighbor group *<1-8>* **shutdown** Enables this peering group configuration. **Command mode:** Router BGP
neighbor group *<1-8>* **shutdown** Disables this peering group configuration. **Command mode:** Router BGP

Table 301. *BGP Peering Group Configuration Options (continued)*

Command Syntax and Usage
neighbor group *<1-8>* **time-to-live** *<number of router hops (1-255)>* Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and must be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded. This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of "hops" the advertisement makes. It is also used to support multi-hops, which allow BGP peering groups to talk across a routed network. The default number is set at `1`. **Note:** The TTL value is significant only to eBGP peering groups; for iBGP peering groups the TTL value in the IP packets is always 255 (regardless of the configured value). **Command mode:** Router BGP
no neighbor group *<1-8>* **time-to-live** *<1-255>* Disables the TTL feature. **Command mode:** Router BGP
neighbor group *<1-8>* **timers hold-time** *<hold time (0, 3-65535)>* Sets the period of time, in seconds, that will elapse before the peering group session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is `180` seconds. **Command mode:** Router BGP
neighbor group *<1-8>* **timers keep-alive** *<keepalive time (0-21845)>* Sets the keep-alive time for the specified peering group in seconds. The default value is `60` seconds. **Command mode:** Router BGP
neighbor group *<1-8>* **ttl-security hops** *<1-254>* Sets the minimum number of time-to-live (TTL) router hops an IP packet must have to not be discarded. **Command mode:** Router BGP
no neighbor group *<1-8>* **ttl-security hops** Disables the TTL security feature. **Command mode:** Router BGP
neighbor group *<1-8>* **update-source {***<interface number (1-126)>***||loopback** *<interface number (1-5)>***}** Sets the local IP interface or loopback interface for this peering group. **Command mode:** Router BGP

Table 301. *BGP Peering Group Configuration Options (continued)*

Command Syntax and Usage
no neighbor group *<1-8>* Deletes this peering group configuration. **Command mode:** Router BGP
show ip bgp neighbor group [*<1-8>***]** Displays the current peering group configuration. **Command mode:** All

BGP Neighbor Group Redistribution Configuration

This menu enables you to redistribute routes learned from various routing information sources into BGP.

Table 302. *BGP Neighbor Redistribution Configuration Options*

Command Syntax and Usage
neighbor group *<1-8>* **redistribute default-action {import|originate|redistribute}** Sets default route action. Defaults routes can be configured as follows: o `import`: Import these routes. o `originate`: The switch sends a default route to peers if it does not have any default routes in its routing table. o `redistribute`: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol. **Command mode:** Router BGP
no neighbor group *<1-8>* **redistribute default-action** Disables the default route action configuration. **Command mode:** Router BGP
neighbor group *<1-8>* **redistribute default-metric** *<1-4294967294>* Sets default metric of advertised routes. **Command mode:** Router BGP
no neighbor group *<1-8>* **redistribute default-metric** Disables the default metric configuration for advertised routes. **Command mode:** Router BGP
[no] neighbor group *<1-8>* **redistribute {fixed|ospf|rip||static}** Enables or disables advertising fixed, OSPF, RIP or static routes. **Command mode:** Router BGP
show ip bgp neighbor group *<1-8>* **redistribute** Displays current redistribution configuration. **Command mode:** All

MLD Global Configuration

The following table describes the commands used to configure global MLD parameters.

Table 303. *MLD Global Configuration Commands*

Command Syntax and Usage
ipv6 mld Enter MLD global configuration mode. **Command mode:** Global configuration
[no] enable Globally enables or disables MLD. **Command mode:** MLD Configuration
default Resets MLD parameters to their default values. **Command mode:** MLD Configuration
show ipv6 mld Displays the current MLD configuration parameters. **Command mode:** All

MLD Interface Configuration

The following table describes the commands used to configure MLD parameters for an interface.

Table 304. *MLD Interface Configuration Commands*

Command Syntax and Usage
`[no] ipv6 mld dmrtr enable` Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled. **Command mode:** Interface IP
`[no] ipv6 mld enable` Enables or disables the selected MLD interface. **Command mode:** Interface IP
`ipv6 mld llistnr` *<1-32>* Configures the Last Listener query interval, in seconds. The default value is `1` second. **Command mode:** Interface IP
`no ipv6 mld llistnr` Resets the Last Listener query interval to its default value of `1` second. **Command mode:** Interface IP
`ipv6 mld qintrval` *<2-65535>* Configures the interval for MLD Query Reports, in seconds. The default value is `125` seconds. **Command mode:** Interface IP
`no ipv6 mld qintrval` Resets the interval for MLD Query Reports to its default value of `125` seconds. **Command mode:** Interface IP
`ipv6 mld qri` *<1000-65535>* Configures the interval for MLD Query Response Reports, in miliseconds. The default value is `10,000` milliseconds. **Command mode:** Interface IP
`no ipv6 mld qri` Resets the interval for MLD Query Response Reports to its default value of `10,000` milliseconds. **Command mode:** Interface IP

Table 304. *MLD Interface Configuration Commands (continued)*

Command Syntax and Usage
ipv6 mld robust *<1-10>* Configures the MLD Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2. **Command mode:** Interface IP
no ipv6 mld robust Resets the MLD Robustness variable to its default value of 2. **Command mode:** Interface IP
ipv6 mld version *<1-2>* Defines the MLD protocol version number. The default value is 1. **Command mode:** Interface IP
no ipv6 mld version Resets the MLD protocol version number to its default value of 1. **Command mode:** Interface IP
ipv6 mld default Resets MLD parameters for the selected interface to their default values. **Command mode:** Interface IP

IGMP Configuration

The following table describes the commands used to configure basic IGMP parameters.

Table 305. *IGMP Configuration Options*

Command Syntax and Usage
`[no] ip igmp aggregate` Enables or disables IGMP Membership Report aggregation. **Command mode:** Global configuration
`[no] ip igmp enable` Globally enables or disables IGMP. **Command mode:** Global configuration
`show ip igmp` Displays the current IGMP configuration parameters. **Command mode:** All

The following sections describe the IGMP configuration options.

- "IGMP Snooping Configuration" on page 581
- "IGMP Relay Configuration" on page 583
- "IGMP Relay Multicast Router Configuration" on page 584
- "IGMP Static Multicast Router Configuration" on page 585
- "IGMP Filtering Configuration" on page 586
- "IGMP Advanced Configuration" on page 588
- "IGMP Querier Configuration" on page 589

IGMP Snooping Configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

The following table describes the commands used to configure IGMP Snooping.

Table 306. *IGMP Snooping Configuration Options*

Command Syntax and Usage
`[no] ip igmp snoop enable` Enables or disables IGMP Snooping. **Command mode:** Global configuration
`[no] ip igmp snoop mrouter-timeout` *<1-600>* Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is `255` seconds. **Command mode:** Global configuration
`[no] ip igmp snoop port` *<port alias or number>* Adds or removes the selected port to/from IGMP Snooping. **Command mode:** Global configuration
`[no] ip igmp snoop source-ip` *<IP address>* Configures the source IP address used as a proxy for IGMP Group Specific Queries. **Command mode:** Global configuration
`ip igmp snoop vlan` *<VLAN ID (1-4094)>* Adds the selected VLAN(s) to IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop vlan {`*<VLAN ID (1-4094)>***`|all}`** Removes all VLANs or just the specified VLAN(s) from IGMP Snooping. **Command mode:** Global configuration
`default ip igmp snoop` Resets IGMP Snooping parameters to their default values. **Command mode:** Global configuration
`show ip igmp snoop` Displays the current IGMP Snooping parameters. **Command mode:** All

IGMPv3 Configuration

The following table describes the commands used to configure IGMP version 3.

Table 307. *IGMP Version 3 Configuration Options*

Command Syntax and Usage
`[no] ip igmp snoop igmpv3 enable` Enables or disables IGMP version 3. The default value is `disabled`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 exclude` Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is `enabled`. **Command mode:** Global configuration
`ip igmp snoop igmpv3 sources` *<1-64>* Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is `8`. **Command mode:** Global configuration
`no ip igmp snoop igmpv3 sources` Resets the maximum number of IGMP multicast sources to snoop from within the group record to its default value of `8`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 v1v2` Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is `enabled`. **Command mode:** Global configuration
`show ip igmp snoop igmpv3` Displays the current IGMP v3 Snooping configuration. **Command mode:** All

IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

The following table describes the commands used to configure IGMP Relay.

Table 308. *IGMP Relay Configuration Options*

Command Syntax and Usage
[no] ip igmp relay enable Enables or disables IGMP Relay. **Command mode:** Global configuration
ip igmp relay report *<0-150>* Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is `10`. **Command mode:** Global configuration
ip igmp relay vlan *<VLAN ID (1-4094)>* Adds the VLAN or range of VLANs to the list of IGMP Relay VLANs. **Command mode:** Global configuration
no ip igmp relay vlan {*<VLAN ID (1-4094)>***|all}** Removes all VLANs or just the specified VLAN from the list of IGMP Relay VLANs. **Command mode:** Global configuration
show ip igmp relay Displays the current IGMP Relay configuration. **Command mode:** All

IGMP Relay Multicast Router Configuration

The following table describes the commands used to configure multicast routers for IGMP Relay.

Table 309. *IGMP Relay Mrouter Configuration Options*

Command Syntax and Usage
ip igmp relay mrouter *<1-2>* **address** *<IP address>* Configures the IP address of the IGMP multicast router used for IGMP Relay. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **attempt** *<1-128>* Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is **5**. **Command mode:** Global configuration
[no] ip igmp relay mrouter *<1-2>* **enable** Enables or disables the multicast router. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **interval** *<1-60>* Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is **2**. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **retry** *<1-120>* Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is **4**. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **version** *<1-2>* Configures the IGMP version (1 or 2) of the multicast router. **Command mode:** Global configuration
no ip igmp relay mrouter *<1-2>* Deletes the multicast router from IGMP Relay. **Command mode:** Global configuration
show ip igmp relay Displays the current IGMP Relay configuration. **Command mode:** All

IGMP Static Multicast Router Configuration

The following table describes the commands used to configure a static multicast router.

Note: When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 310. *IGMP Static Multicast Router Configuration Options*

Command Syntax and Usage
ip igmp mrouter port *<port alias or number> <VLAN ID (1-4094)> <version (1-3)>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version of the multicast router. **Command mode:** Global configuration
no ip igmp mrouter {port *<port alias or number> <VLAN ID (1-4094)> <version (1-3)>***|all}** Removes all static multicast routers or a specific static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
clear ip igmp mrouter Clears the dynamic multicast router port table. **Command mode:** Privileged EXEC
show ip igmp mrouter Displays the current IGMP Multicast Router parameters. **Command mode:** All

IGMP Filtering Configuration

The following table describes the commands used to configure an IGMP filter.

Table 311. *IGMP Filtering Configuration Options*

Command Syntax and Usage
ip igmp profile *<1-16>* Configures the IGMP filter. To view command options, see page 586. **Command mode:** Global configuration
[no] ip igmp filtering Enables or disables IGMP filtering globally. **Command mode:** Global configuration
show ip igmp filtering Displays the current IGMP Filtering parameters. **Command mode:** All

IGMP Filter Definition

The following table describes the commands used to define an IGMP filter.

Table 312. *IGMP Filter Definition Options*

Command Syntax and Usage
ip igmp profile *<1-16>* **action {allow|deny}** Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny. **Command mode:** Global configuration
[no] ip igmp profile *<1-16>* **enable** Enables or disables this IGMP filter. **Command mode:** Global configuration
ip igmp profile *<1-16>* **range** *<IP address 1> <IP address 2>* Configures the range of IP multicast addresses for this filter. **Command mode:** Global configuration
no ip igmp profile *<1-16>* Deletes this filter's parameter definitions. **Command mode:** Global configuration
show ip igmp profile *<1-16>* Displays the current IGMP filter. **Command mode:** All

IGMP Filtering Port Configuration

The following table describes the commands used to configure a port for IGMP filtering.

Table 313. *IGMP Filter Port Configuration Options*

Command Syntax and Usage
`[no] ip igmp filtering` Enables or disables IGMP filtering on this port. **Command mode:** Interface port
`[no] ip igmp profile` *<1-16>* Adds or removes an IGMP filter to this port. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`igmp-filtering`** Displays the current IGMP filter parameters for this port. **Command mode:** All

IGMP Advanced Configuration

The following table describes the commands used to configure advanced IGMP parameters.

Table 314. *IGMP Advanced Configuration Options*

Command Syntax and Usage
[no] ip igmp fastleave {<*VLAN ID (1-4094)*>**|port** <*port alias or number*>**}** Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a VLAN from the IGMP VLAN list or a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is `disabled` by default. **Command mode:** Global configuration
ip igmp query-interval <*1-600*> Sets the IGMP router query interval, in seconds. The default value is `125` seconds. **Command mode:** Global configuration
no ip igmp query-interval Resets the IGMP router query interval to its default value of `125` seconds. **Command mode:** Global configuration
ip igmp robust <*1-10*> Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is `2`. **Command mode:** Global configuration
no ip igmp robust Resets the IGMP Robustness variable to its default value of `2`. **Command mode:** Global configuration
[no] ip igmp rtralert Enables or disables the Router Alert option in IGMP messages. **Command mode:** Global configuration

Table 314. *IGMP Advanced Configuration Options (continued)*

Command Syntax and Usage
ip igmp timeout *<1-255>* Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is `10` seconds. **Command mode:** Global configuration
no ip igmp timeout Resets the timeout value for IGMP Membership Reports (host) to its default value of `10` seconds. **Command mode:** Global configuration

IGMP Querier Configuration

The following table describes the commands used to configure IGMP Querier.

Table 315. *IGMP Querier Configuration Options*

Command Syntax and Usage
[no] ip igmp querier enable Enables or disables IGMP Querier. **Command mode:** Global configuration
[no] ip igmp querier port *<port alias or number>* Adds or removes the specified port to/from IGMP Querier. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **election-type {ipv4|mac}** Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is `ipv4`. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **election-type** Resets the IGMP Querier election criteria to its default value - `ipv4`. **Command mode:** Global configuration
[no] ip igmp querier vlan *<VLAN ID (1-4094)>* **enable** Enables or disables IGMP Querier for the selected VLANs. **Command mode:** Global configuration

Table 315. *IGMP Querier Configuration Options (continued)*

Command Syntax and Usage
ip igmp querier vlan *<VLAN ID (1-4094)>* **max-response** *<1-256>* Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is `100`. By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **max-response** Resets the maximum time allowed before responding to a Membership Query message to its default value of `100`. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **query-interval** *<1-608>* Configures the interval between IGMP Query broadcasts. The default value is `125` seconds. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **query-interval** Resets the interval between IGMP Query broadcasts to its default value of `125` seconds. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **robustness** *<1-10>* Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is `2`. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **robustness** Resets the IGMP Robustness variable to its default value of `2`. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **source-ip** *<IP address>* Configures the IGMP source IP address for the selected VLAN. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **source-ip** Removes the configured IGMP source IP address for the specified VLAN. **Command mode:** Global configuration

Table 315. *IGMP Querier Configuration Options (continued)*

Command Syntax and Usage
ip igmp querier vlan *<VLAN ID (1-4094)>* **startup-count** *<1-10>* Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **startup-count** Resets the Startup Query Count to its default value of 2. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **startup-interval** *<1-608>* Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. The default value is 31 seconds. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **startup-interval** Resets the Startup Query Interval to its default value of 31 seconds. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN ID (1-4094)>* **version {v1|v2|v3}** Configures the IGMP version. The default version is v3. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* **version** Resets the IGMP version to its default value of v3. **Command mode:** Global configuration
no ip igmp querier vlan *<VLAN ID (1-4094)>* Deletes the IGMP Querier configuration for the specified VLAN. **Command mode:** Global configuration
show ip igmp querier Displays the current IGMP Querier parameters. **Command mode:** All
show ip igmp querier vlan *<VLAN ID (1-4094)>* Displays IGMP Querier information for the selected VLAN. **Command mode:** Global configuration

IKEv2 Configuration

The following table describes the commands used to configure IKEv2.

Table 316. *IKEv2 Options*

Command Syntax and Usage
`[no] ikev2 cookie` Enables or disables cookie notification. **Command mode:** Global configuration
`ikev2 retransmit-interval` *<1-20>* Sets the interval, in seconds, the timeout value in case a packet is not received by the peer and needs to be retransmitted. The default value is `20` seconds. **Command mode:** Global configuration
`show ikev2` Displays the current IKEv2 settings. **Command mode:** All

IKEv2 Preshare Key Configuration

The following table describes the commands used to configure IKEv2 preshare keys.

Table 317. *IKEv2 Preshare Key Options*

Command Syntax and Usage
`ikev2 preshare-key local` *<1-256 characters>* Configures the local preshare key. The default value is `ibm123`. **Command mode:** Global configuration
`ikev2 preshare-key remote` *<1-256 characters> <IPv6 address>* Configures the remote preshare key for the IPv6 address. **Command mode:** Global configuration
`show ikev2 preshare-key` Displays the current IKEv2 Preshare key settings. **Command mode:** Global configuration

IKEv2 Proposal Configuration

The following table describes the commands used to configure an IKEv2 proposal.

IKEv2 proposal includes an encryption algorithm (cipher), an authentication algorithm type and a Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. Higher DH group numbers are more secure but require additional time to compute the key.

Table 318. *IKEv2 Proposal Options*

Command Syntax and Usage
ikev2 proposal Enter IKEv2 proposal mode. **Command mode:** Global configuration
encryption {3des|aes-cbc} Configures IKEv2 encryption mode. The default value is `3des`. **Command mode:** IKEv2 proposal
group 24 Configures the DH group. The default group is `2`. **Command mode:** IKEv2 proposal
integrity sha1 Configures the IKEv2 authentication algorithm type. The default value is `sha1`. **Command mode:** IKEv2 proposal
show ikev2 proposal Displays the current IKEv2 Proposal configuration. **Command mode:** All

IKEv2 Identification Configuration

The following table describes the commands used to configure IKEv2 identification.

Table 319. *IKEv2 Identification Options*

Command Syntax and Usage
ikev2 identity local address Configures the switch to use the supplied IPv6 address as identification. **Command mode:** Global configuration
ikev2 identity local fqdn *<1-32 characters>* Configures the switch to use the fully-qualified domain name (such as "example.com") as identification. **Command mode:** Global configuration
ikev2 identity local email *<1-32 characters>* Configures the switch to use the supplied email address (such as "`xyz@example.com`") as identification. **Command mode:** Global configuration
show ikev2 identity Displays the current IKEv2 identification settings. **Command mode:** All

IPsec Configuration

The following table describes the commands used to configure IPsec.

Table 320. *IPsec Options*

Command Syntax and Usage
[no] ipsec enable Enables or disables IPsec. **Command mode:** Global configuration
show ipsec Displays the current IPsec settings. **Command mode:** All

IPsec Transform Set Configuration

The following table describes the commands used to configure IPsec transforms.

Table 321. *IPsec Transform Set Options*

Command Syntax and Usage
ipsec transform-set *<1-10>* **{ah-sha1|esp-3des|esp-aes-cbc| |esp-null|esp-sha1}** Sets the AH or ESP authentication, encryption, or integrity algorithm. The available algorithms are as follows: o ah-sha1 o esp-3des o esp-aes-cbc o esp-null o esp-sha1 **Command mode:** Global configuration
ipsec transform-set *<1-10>* **transport {ah-sha1|esp-3des| |esp-aes-cbc|esp-null|esp-sha1}** Sets transport mode and the AH or ESP authentication, encryption, or integrity algorithm. **Command mode:** Global configuration
ipsec transform-set *<1-10>* **tunnel {ah-sha1|esp-3des| |esp-aes-cbc|esp-null|esp-sha1}** Sets tunnel mode and the AH or ESP authentication, encryption, or integrity algorithm. **Command mode:** Global configuration

Table 321. *IPsec Transform Set Options (continued)*

Command Syntax and Usage
no ipsec transform *<1-10>* Deletes the transform set. **Command mode:** Global configuration
show ipsec transform-set *<1-10>* Displays the current IPsec Transform Set settings. **Command mode:** All

IPsec Traffic Selector Configuration

The following table describes the commands used to configure an IPsec traffic selector.

Table 322. *IPsec Traffic Selector Options*

Command Syntax and Usage
ipsec traffic-selector *<1-10>* **{permit|deny} {any|icmp [***<ICMPv6 type (0-255)>***]|tcp} {***<IPV6 address>***|any}** Sets the traffic-selector to permit or deny the specified type of traffic. **Command mode:** Global configuration
no ipsec traffic-selector *<1-10>* Resets the specified traffic selector to its default values. **Command mode:** Global configuration
show ipsec traffic-selector [*<1-10>***]** Displays IPsec traffic selector information. **Command mode:** All

IPsec Dynamic Policy Configuration

The following table describes the commands used to configure an IPsec dynamic policy.

Table 323. *IPsec Dynamic Policy Options*

Command Syntax and Usage
ipsec dynamic-policy *<1-10>* Enter IPsec dynamic policy mode. **Command mode:** Global configuration
peer *<IPv6 address>* Sets the remote peer IP address. **Command mode:** IPsec dynamic policy
pfs {enable|disable} Enables or disables perfect forward security. **Command mode:** IPsec dynamic policy
sa-lifetime *<120-86400>* Sets the IPsec SA lifetime in seconds. The default value is **86400** seconds. **Command mode:** IPsec dynamic policy
traffic-selector *<1-10>* Sets the traffic selector for the IPsec policy. **Command mode:** IPsec dynamic policy
transform-set *<1-10>* Sets the transform set for the IPsec policy. **Command mode:** IPsec dynamic policy
show ipsec dynamic-policy *<1-10>* Displays the current IPsec dynamic policy settings. **Command mode:** All

IPsec Manual Policy Configuration

The following table describes the commands used to configure an IPsec manual policy.

Table 324. *IPsec Manual Policy Options*

Command Syntax and Usage
ipsec manual-policy *<1-10>* Enter IPsec manual policy mode. **Command mode:** Global configuration
in-ah auth-key *<key code (hexadecimal)>* Sets inbound Authentication Header (AH) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy
in-ah spi *<256-4294967295>* Sets the inbound Authentication Header (AH) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy
in-esp {auth-key|cipher-key} *<key code (hexadecimal)>* Sets the inbound Encapsulating Security Payload (ESP) authenticator key or cipher key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy
in-esp spi *<256-4294967295>* Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy
out-ah auth-key *<key code (hexadecimal)>* Sets the outbound Authentication Header (AH) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy

Table 324. *IPsec Manual Policy Options (continued)*

Command Syntax and Usage
out-ah spi *<256-4294967295>* Sets the outbound Authentication Header (AH) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy
out-esp {auth-key|cipher-key} *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) authenticator key or cipher key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy
out-esp spi *<256-4294967295>* Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1. **Command mode:** IPsec manual policy
peer *<IPv6 address>* Sets the remote peer IP address. **Command mode:** IPsec manual policy
traffic-selector *<1-10>* Sets the traffic selector for the IPsec policy. **Command mode:** IPsec manual policy
transform-set *<1-10>* Sets the transform set for the IPsec policy. **Command mode:** IPsec manual policy
show ipsec manual-policy *<1-10>* Displays the current IPsec manual policy settings. **Command mode:** All

Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 325. *Domain Name Service Options*

Command Syntax and Usage
`ip dns domain-name` *<1-191 characters>* Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
`no ip dns domain-name` Removes the domain name used by the switch. **Command mode:** Global configuration
`ip dns primary-server` *<IPv4 address>* **`[data-port|mgt-port]`** You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation. **Command mode:** Global configuration
`no ip dns primary-server` Removes the IPv4 primary DNS server. **Command mode:** Global configuration
`ip dns secondary-server` *<IPv4 address>* **`[data-port|mgt-port]`** You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
`no ip dns secondary-server` Removes the IPv4 secondary DNS server. **Command mode:** Global configuration
`ip dns ipv6 primary-server [`*<IPv6 address>***`] [data-port| |mgt-port]`** You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons. **Command mode:** Global configuration
`no ip dns ipv6 primary-server` Removes the IPv6 primary DNS server. **Command mode:** Global configuration

Table 325. *Domain Name Service Options*

Command Syntax and Usage
ip dns ipv6 secondary-server [<*IPv6 address*>**] [data-port| |mgt-port]** You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
no ip dns ipv6 secondary-server Removes the IPv6 secondary DNS server. **Command mode:** Global configuration
ip dns ipv6 request-version {ipv4|ipv6} Sets the protocol used for the first request to the DNS server, as follows: o IPv4 o IPv6 **Command mode:** Global configuration
show ip dns Displays the current Domain Name System settings. **Command mode:** All

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to DHCP/BOOTP servers with IP addresses that have been configured on the G8272.

BOOTP relay is turned off by default.

Table 326. *Global BOOTP Relay Configuration Options*

Command Syntax and Usage
[no] ip bootp-relay enable Globally enables or disables BOOTP relay. **Command mode:** Global configuration
ip bootp-relay server <*1-5*> **address** <*IP address*> Sets the IP address of the selected global BOOTP server. **Command mode:** Global configuration
no ip bootp-relay server <*1-5*> Removes the specified BOOTP server. **Command mode:** Global configuration

BOOTP Relay Broadcast Domain Configuration

This menu allows you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

Table 327. *BOOTP Relay Broadcast Domain Configuration Options*

Command Syntax and Usage
[no] ip bootp-relay bcast-domain *<1-10>* **enable** Enables or disables BOOTP Relay for the broadcast domain. **Command mode:** Global configuration
ip bootp-relay bcast-domain *<1-10>* **server** *<1-5>* **address** *<IPv4 address>* Sets the IP address of the BOOTP server. **Command mode:** Global configuration
no ip bootp-relay bcast-domain *<1-10>* **server** *<1-5>* Removes the broadcast domain BOOTP server. **Command mode:** Global configuration
ip bootp-relay bcast-domain *<1-10>* **vlan** *<VLAN ID (1-4094)>* Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN. **Command mode:** Global configuration

Table 327. *BOOTP Relay Broadcast Domain Configuration Options (continued)*

Command Syntax and Usage
no ip bootp-relay bcast-domain *<1-10>* Deletes the selected broadcast domain configuration. **Command mode:** Global configuration
show ip bootp-relay Displays the current parameters for the BOOTP Relay broadcast domain. **Command mode:** All

Option 82 Configuration

These commands allow you to configure DHCP option 82 information. The switch can use the following DHCP option 82 sub-options to allocate server addresses.

- Circuit ID: Identifies the host name or MAC addresses of the switch making the DHCP request.
- Remote ID: Identifies the port that receives the DHCP request.

DHCP Relay Agent (Option 82) is defined in RFC 3046.

Table 328. *Option 82 Configuration Options*

Command Syntax and Usage
[no] ip bootp-relay information enable Enables or disables BOOTP Option 82. **Command mode:** Global configuration
ip bootp-relay information policy {keep|drop|replace} Configures the DHCP re-forwarding policy, as follows: o `keep`: Retains requests that contain relay information if the option 82 information is also present. o `drop`: Discards requests that contain relay information if the option 82 information is also present. o `replace`: Replaces the relay information in requests that also contain option 82 information. **Command mode:** Global configuration
no ip bootp-relay information policy Removes the DHCP re-forwarding policy. **Command mode:** Global configuration
show ip bootp-relay Displays the current BOOTP Option 82 parameters. **Command mode:** All

VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on the G8272 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. Enterprise NOS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the "High Availability" chapter in the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

Table 329. *Virtual Router Redundancy Protocol Options*

Command Syntax and Usage
`router vrrp` Enter Router VRRP configuration mode. **Command mode:** Global configuration
`[no] enable` Globally enables or disables VRRP on this switch. **Command mode:** Router VRRP
`group` Configures VRRP virtual routers groups. To view command options, see page 610. **Command mode:** Router VRRP
`holdoff` *<0-255>* Globally sets the time, in seconds, that VRRP waits from when the master switch goes down until elevating a new switch to be the master switch. To disable VRRP hold off set the time to `0`. **Note:** Setting a new time value will take effect only when the switch is not in a hold off state. **Command mode:** Router VRRP
`interface` *<1-126>* Configures VRRP authentication parameters for the IP interfaces used with the virtual routers. To view command options, see page 614. **Command mode:** Router VRRP
`tracking-priority-increment` Configures weights for the various criteria used to modify priority levels during the master router election process. To view command options, see page 615. **Command mode:** Router VRRP

Table 329. *Virtual Router Redundancy Protocol Options*

Command Syntax and Usage
virtual-router *<1-128>* Configures virtual routers for the switch. To view command options, see page 606. **Command mode:** Router VRRP
show ip vrrp Displays the current VRRP parameters. **Command mode:** All

Virtual Router Configuration

These commands are used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 330. *VRRP Virtual Router Configuration Options*

Command Syntax and Usage
virtual-router *<1-128>* **address** *<IP address>* Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the preceding VRID to configure the same virtual router on each participating VRRP device. The default address is `0.0.0.0`. **Command mode:** Router VRRP
[no] virtual-router *<1-128>* **enable** Enables or disables this virtual router. **Command mode:** Router VRRP
[no] virtual-router *<1-128>* **fast-advertise** Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if `adver` is set to 1 and `fadver` is enabled, master advertisements are sent every 10 miliseconds. When you disable fast advertisement, the advertisement interval is set to the default value of `1` second. To support Fast Advertisements, set the interval between 20-100 centiseconds. **Command mode:** Router VRRP
virtual-router *<1-128>* **interface** *<IP interface number>* Selects a switch IP interface. If the IP interface has the same IP address as the `address` option, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the `preem` option below is disabled. The default value is `1`. **Command mode:** Router VRRP

Table 330. *VRRP Virtual Router Configuration Options (continued)*

Command Syntax and Usage
virtual-router *<1-128>* **next-hop** *<IP address>* **[arp|icmp] [interval** *<1-60>***] [retry** *<1-3>***]** Defines the next-hop IP address and tracking parameters. If not successful, the command will retry the health check at regular intervals of the specified number of seconds for the number of retries specified by `retry`. Default values are `icmp`, `2` seconds and `3` retries. **Note:** Up to 4 unique next-hops can be configured for a virtual router. All 4 next-hops will be tracked. **Command mode:** Router VRRP
no virtual-router *<1-128>* **next-hop** *<IP address>* Removes the specified next-hop IP address. **Command mode:** Router VRRP
[no] virtual-router *<1-128>* **preemption [priority-only]** Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is `enabled`. If `priority-only` is specified, preemption is based on priority and the IP address is disregarded. **Command mode:** Router VRRP
virtual-router *<1-128>* **priority** *<1-254>* Defines the election priority bias for this virtual server. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria. The priority value can be any integer between 1 and 254. The default value is `100`. **Command mode:** Router VRRP
virtual-router *<1-128>* **timers advertise** *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is `1`. **Command mode:** Router VRRP

Table 330. *VRRP Virtual Router Configuration Options (continued)*

Command Syntax and Usage
virtual-router *<1-128>* **timers preempt-delay-time** *<0-255>* Configures the preempt delay interval (in seconds). This timer is configured on the virtual router and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge. The default is `0` seconds. **Command mode:** Router VRRP
virtual-router *<1-128>* **track** Enables the priority system used when electing the master router from a pool of virtual routers. To view command options, see page 609. **Command mode:** Router VRRP
virtual-router *<1-128>* **virtual-router-id** *<1-128>* Defines the virtual router ID (VRID). This is used in conjunction with the `[no] virtual-router` *<VRID>* `address` *<IP address>* command below to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router. The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 128. The default value is `1`. **Note:** All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs. **Command mode:** Router VRRP
no virtual-router *<1-128>* Deletes this virtual router from the switch configuration. **Command mode:** Router VRRP
show ip vrrp virtual-router *<1-128>* Displays the current configuration information for this virtual router. **Command mode:** All

Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called "virtual interface routers." A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 331. *VRRP Priority Tracking Configuration Options*

Command Syntax and Usage
`[no] virtual-router` *<1-128>* **`track interfaces`** When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is `disabled` by default. **Command mode:** Router VRRP
`[no] virtual-router` *<1-128>* **`track next-hops`** When enabled, the priority for this virtual router will be increased for all active next hops. A next-hop is considered active if it is configured. This command is `disabled` by default. **Command mode:** Router VRRP
`[no] virtual-router` *<1-128>* **`track ports`** When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is `disabled` by default. **Command mode:** Router VRRP

Table 331. *VRRP Priority Tracking Configuration Options*

Command Syntax and Usage
`[no] virtual-router` *<1-128>* **`track virtual-routers`** When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is `disabled` by default. **Command mode:** Router VRRP
`show ip vrrp virtual-router` *<1-128>* **`track`** Displays the current configuration for priority tracking for this virtual router. **Command mode:** All

Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the G8272 to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note: This option is required to be configured only when using at least two G8272s in a hot-standby failover configuration, where only one switch is active at any time.

Table 332. *VRRP Virtual Router Group Configuration Options*

Command Syntax and Usage
`group advertisement` *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is `1`. **Command mode:** Router VRRP
`[no] group enable` Enables or disables the virtual router group. **Command mode:** Router VRRP
`[no] group fast-advertise` Enables or disables Fast Advertisements. When enabled, the VRRP master advertisements interval is calculated in units of centiseconds, instead of seconds. For example, if `adver` is set to 1 and `fadver` is enabled, master advertisements are sent every 10 miliseconds. When you disable fast advertisement, the advertisement interval is set to the default value of `1` second. To support Fast Advertisements, set the interval between 20-100 centiseconds. **Command mode:** Router VRRP

Table 332. *VRRP Virtual Router Group Configuration Options (continued)*

Command Syntax and Usage
group interface *<interface number (1-126)>* Selects a switch IP interface. The default switch IP interface number is `1`. **Command mode:** Router VRRP
group interface *<interface number (1-126)>* **restricted** Enables restricted VRRP control traffic on an interface. When enabled, the VRRP control messages can be sent to a dedicated interface only. This helps preventing control messages from being dropped. **Command mode:** Router VRRP
group preempt-delay-time *<0-255>* Configures the preempt delay interval (in seconds). This timer is configured on the virtual router group and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge. The default value is `0` seconds. **Command mode:** Router VRRP
[no] group preemption [priority-only] Enables or disables master pre-emption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will pre-empt the lower priority master and assume control. Note that even when `preemption` is disabled, this virtual router will always pre-empt any other master if this switch is the owner (the IP interface address and virtual router address are the same). The default setting is `enabled`. If `priority-only` is specified, preemption is based on priority and the IP address is disregarded. **Command mode:** Router VRRP
group priority *<1-254>* Defines the election priority bias for this virtual router group. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). This can be any integer between 1 and 254. The default value is `100`. When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria. **Command mode:** Router VRRP

Table 332. *VRRP Virtual Router Group Configuration Options (continued)*

Command Syntax and Usage
`group track` Enables the priority system used when electing the master router from a pool of virtual router groups. To view command options, see page 613. **Command mode:** Router VRRP
`group virtual-router-id` *<1-255>* Defines the virtual router ID (VRID). The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 128. All VRID values must be unique within the VLAN to which the virtual router's IP interface (see `interface`) belongs. The default virtual router ID is `1`. **Command mode:** Router VRRP
`no group` Deletes the virtual router group from the switch configuration. **Command mode:** Router VRRP
`show ip vrrp group` Displays the current configuration information for the virtual router group. **Command mode:** All

Note: If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 333. *Virtual Router Group Priority Tracking Configuration Options*

Command Syntax and Usage
`[no] group track interfaces` When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is `disabled` by default. **Command mode:** Router VRRP
`[no] group track ports` When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is `disabled` by default. **Command mode:** Router VRRP
`show ip vrrp group track` Displays the current configuration for priority tracking for this virtual router. **Command mode:** All

VRRP Interface Configuration

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Note: The *interface* represents the IP interface on which authentication parameters must be configured.

Table 334. *VRRP Interface Options*

Command Syntax and Usage
`interface` *<1-126>* **`authentication {password|none}`** Defines the type of authentication that will be used: o `none` (no authentication) o `password` (password authentication). **Command mode:** Router VRRP
`interface` *<1-126>* **`password`** *<password>* Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see `interface authentication` above). **Command mode:** Router VRRP
`no interface` *<1-126>* **`password`** Resets the configured password to its default value. **Command mode:** Router VRRP
`no interface` *<1-126>* Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted. **Command mode:** Router VRRP
`show ip vrrp interface` *<1-126>* Displays the current configuration for this IP interface's authentication parameters. **Command mode:** All

VRRP Tracking Configuration

These commands are used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see "VRRP Virtual Router Priority Tracking Commands" on page 609), the priority level for the virtual router is increased by a defined amount.

Table 335. *VRRP Tracking Configuration Options*

Command Syntax and Usage
tracking-priority-increment interfaces *<0-254>* Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2. **Command mode:** Router VRRP
tracking-priority-increment next-hops *<0-254>* Defines the priority increment value for each next-hop that is active or subtracted. The default value is 2. **Command mode:** Router VRRP
tracking-priority-increment ports *<0-254>* Defines the priority increment value for active ports on the virtual router's VLAN. The default value is 2. **Command mode:** Router VRRP
tracking-priority-increment virtual-routers *<0-254>* Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2. **Command mode:** Router VRRP
show ip vrrp tracking-priority-increment Displays the current configuration of priority tracking increment values. **Command mode:** All

Note: These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see page 609) are enabled.

Protocol Independent Multicast Configuration

The following table describes the PIM commands.

Table 336. *PIM Configuration Options*

Command Syntax and Usage
ip pim component *<1-2>* Enter PIM component mode. **Command mode**: Global configuration
no ip pim component *<2>* Deletes the PIM component. **Command mode:** Global configuration
[no] ip pim enable Globally enables or disables PIM. **Command mode**: Global configuration
[no] ip pim pmbr enable Enables or disables PIM border router. The default setting is `disabled`. **Command mode**: Global configuration
ip pim regstop-ratelimit-period *<0-2147483647>* Configures the register stop rate limit, in seconds. The default value is `5` seconds. **Command mode**: Global configuration
default ip pim regstop-ratelimit-period Reset the register stop rate limit to its default value of `5` seconds. **Command mode:** Global configuration
no ip pim regstop-ratelimit-period Disables the register stop rate limit. **Command mode:** Global configuration
[no] ip pim static-rp enable Enables or disables static RP configuration. The default setting is `disabled`. **Command mode**: Global configuration

Table 336. *PIM Configuration Options*

Command Syntax and Usage
default ip pim Resets the PIM configuration to its default values. **Command mode:** Global configuration
clear ip pim mroute Clears PIM multicast router entries. **Command mode**: Privileged EXEC

PIM Component Configuration

Use these commands to configure PIM components.

Table 337. *PIM Component Configuration Options*

Command Syntax and Usage
ip pim component *<1-2>* Enter PIM component mode. **Command mode**: Global configuration
mode {dense|sparse} Configures the operational mode of the PIM router (dense or sparse). **Command mode**: PIM Component
show ip pim component [*<1-2>***]** Displays the current PIM component configuration settings. **Command mode**: All

RP Candidate Configuration

Use these commands to configure a PIM router Rendezvous Point (RP) candidate.

Table 338. *RP Candidate Configuration Options*

Command Syntax and Usage
rp-candidate holdtime *<0-255>* Configures the hold time of the RP candidate, in seconds. **Command mode**: PIM Component
no rp-candidate holdtime Resets the hold time of the RP candidate to its default value of `0` seconds. **Command mode:** PIM Component
[no] rp-candidate rp-address *<group multicast address> <group subnet mask> <IP address>* Adds or removes an RP candidate. **Command mode**: PIM Component

RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

Table 339. *RP Static Configuration Options*

Command Syntax and Usage
rp-static rp-address *<group multicast address> <group subnet mask> <IP address>* Adds a static RP. **Command mode**: PIM Component
no rp-static rp-address *<group multicast address> <group subnet mask>* Removes the specified static RP. **Command mode**: PIM Component

PIM Interface Configuration

The following table describes the PIM Interface commands.

Table 340. *PIM Interface Configuration Options*

Command Syntax and Usage
interface ip *<1-128>* Enter Interface IP mode. **Command mode**: Global Configuration
[no] ip pim border-bit Enables or disables the interface as a border router. The default setting is `disabled`. **Command mode**: Interface IP
ip pim cbsr-preference *<0-255>* Configures the candidate bootstrap router preference. **Command mode**: Interface IP
[default|no] ip pim cbsr-preference Resets the canditate bootstrap router preference to its default value. **Command mode:** Interface IP
ip pim component-id *<1-2>* Defines the component ID for the interface. **Command mode**: Interface IP
no ip pim component-id Removes the interface from the PIM component. **Command mode:** Interface IP
ip pim dr-priority *<0-4294967294>* Configures the designated router priority. The default value is `1`. **Command mode**: Interface IP
[default|no] ip pim dr-priority Resets the designated router priority to its default value of `1`. **Command mode:** Interface IP
[no] ip pim enable Enables or disables PIM on the interface. **Command mode**: Interface IP

Table 340. *PIM Interface Configuration Options (continued)*

Command Syntax and Usage
ip pim hello-holdtime *<1-65535>* Configures the time period in seconds for which a neighbor is to consider this switch to be operative (up). The default value is `105` seconds. **Command mode**: Interface IP
[default|no] ip pim hello-holdtime Resets the PIM Hello packets hold time to its default value of `105` seconds. **Command mode:** Interface IP
ip pim hello-interval *<0-65535>* Configures the time interval, in seconds, between PIM Hello packets. The default value is `30` seconds. **Command mode**: Interface IP
[default|no] ip pim hello-interval Resets the time interval between PIM Hello packets to its default value of `30` seconds. **Command mode:** Interface IP
ip pim join-prune-interval *<0-65535>* Configures the interval between Join Prune messages, in seconds. The default value is `60` seconds. **Command mode**: Interface IP
[default|no] ip pim join-prune-interval Resets the interval between Join Prune messages to its default value of `60` seconds. **Command mode:** Interface IP
ip pim lan-delay *<0-32767>* Configures the LAN delay value for the router interface, in seconds. **Command mode**: Interface IP
[default|no] ip pim lan-delay Resets the LAN delay for the router interface to its default value. **Command mode:** Interface IP
[no] ip pim lan-prune-delay Enables or disables LAN delay advertisements on the interface. The default setting is `disabled`. **Command mode**: Interface IP

Table 340. *PIM Interface Configuration Options (continued)*

Command Syntax and Usage
ip pim neighbor-addr *<IP address>* **{allow|deny}** Allows or denies PIM access to the specified neighbor. You can configure a list of up to 72 neighbors that bypass the neighbor filter. Once you configure the interface to allow a neighbor, you can configure the interface to deny the neighbor. **Command mode**: Interface IP
[no] ip pim neighbor-filter Enables or disables the PIM neighbor filter on the interface. When enabled, this interface does not accept any PIM neighbors, unless specifically permitted using the following command: **ip pim neighbor-addr** *<IP address>* **Command mode**: Interface IP
ip pim override-interval *<0-65535>* Configures the override interval for the router interface, in seconds. **Command mode**: Interface IP
[default|no] ip pim override-interval Resets the override interval for the router interface to its default value. **Command mode:** Interface IP
default ip pim Resets the PIM configuration on the interface to its default values. **Command mode:** Interface IP
show ip pim neighbor-filters Displays the configured PIM neighbor filters. **Command mode**: All
show ip pim interface [*<1-126>***|detail|loopback** *<1-5>***|port** *<port alias or number>***]** Displays the current PIM interface parameters. **Command mode**: All

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways, as follows:

- Gateway 1: data traffic
- Gateway 4: management port

The following table describes the IPv6 Default Gateway Configuration commands.

Table 341. *IPv6 Default Gateway Configuration Options*

Command Syntax and Usage
ip gateway6 {*1***|***4***} address** *<IPv6 address>* **[enable]** Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as `3001:0:0:0:0:0:abcd:12`). The `enable` option also enables the gateway. **Command mode**: Global configuration
[no] ip gateway6 {*1***|***4***} enable** Enables or disables the default gateway. **Command mode**: Global configuration
no ip gateway6 {*1***|***4***}** Deletes the default gateway. **Command mode**: Global configuration
show ipv6 gateway6 {*1***|***4***}** Displays the current IPv6 default gateway configuration. **Command mode**: All

IPv6 Static Route Configuration

The following table describes the IPv6 static route configuration commands.

Table 342. *IPv6 Static Route Configuration Options*

Command Syntax and Usage
ip route6 *<IPv6 address> <IPv6 prefix length> <IPv6 gateway address>* **[***<interface number (1-126)>***]** Adds an IPv6 static route. **Command mode**: Global configuration
no ip route6 *<IPv6 address> <IPv6 prefix length>* **[***<IP interface number>***]** Removes the selected route. **Command mode**: Global configuration
no ip route6 [destination-address *<IPv6 address>***|gateway** *<default IPv6 gateway address>***|interface** *<IP interface number>***|all]** Clears the selected IPv6 static routes. **Command mode**: Global configuration
show ipv6 route static Displays the current static route configuration. **Command mode**: All

IPv6 Neighbor Discovery Cache Configuration

The following table describes the IPv6 Neighbor Discovery cache configuration commands.

Table 343. *IPv6 Neighbor Discovery Cache Configuration Options*

Command Syntax and Usage
ip neighbors *<IPv6 address> <MAC address>* **vlan** *<VLAN ID (1-4094)>* **port** *<port number or alias>* Adds a static entry to the Neighbor Discovery cache table. **Command mode**: Global configuration
no ip neighbors *<IPv6 address>* Deletes the selected entry from the static Neighbor Discovery cache table. **Command mode**: Global configuration
no ip neighbors all [ip *<IP interface number>***|interface port** *<port alias or number>***|vlan** *<VLAN ID (1-4094)>***]** Clears the selected static entries in the Neighbor Discovery cache table. **Command mode**: Global configuration

IPv6 Path MTU Configuration

The following table describes the configuration options for Path MTU (Maximum Transmission Unit). The Path MTU cache can consume system memory and affect performance. These commands allow you to manage the Path MTU cache.

Table 344. *IPv6 Path MTU Options*

Command Syntax and Usage
ip pmtu6 timeout {*0***|***<10-100>***}** Sets the timeout value for Path MTU cache entries, in minutes. Enter `0` (zero) to set the timeout to infinity (no timeout). The default value is `10` minutes. **Command mode**: Global configuration
clear ipv6 pmtu Clears all entries in the Path MTU cache. **Command mode**: Privileged EXEC
show ipv6 pmtu Displays the current Path MTU configuration. **Command mode**: All

IPv6 Neighbor Discovery Prefix Configuration

The following table describes the Neighbor Discovery prefix configuration options. These commands allow you to define a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from an interface.

Table 345. *IPv6 Neighbor Discovery Prefix Options*

Command Syntax and Usage
interface ip *<1-128>* Enters Interface IP mode. **Command mode**: Global configuration
ipv6 nd prefix *<IPv6 prefix> <IPv6 prefix length>* **[no-advertise]** Adds a Neighbor Discovery prefix to the interface. The default setting is `enabled`. To disable the prefix and not advertise it in the Prefix Information options in Router Advertisement messages sent from the interface use the `no-advertise` option. Additional prefix options are listed below. **Command mode**: Interface IP

Table 345. *IPv6 Neighbor Discovery Prefix Options (continued)*

Command Syntax and Usage
no ipv6 nd prefix {*<IPv6 prefix> <IPv6 prefix length>***|interface** *<IP interface number>***|all}** Removes a Neighbor Discovery prefix. If you specify an interface number, all prefixes for the interface are removed. **Command mode**: Interface IP
ipv6 nd prefix *<IPv6 prefix> <IPv6 prefix length>* **no-autoconfig** Disables the autonomous flag. When enabled, the autonomous flag indicates that the prefix can be used for stateless address configuration. The default setting is `enabled`. **Command mode**: Interface IP
ipv6 nd prefix *<IPv6 prefix> <IPv6 prefix length>* **off-link** Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix. The default setting is `enabled`. To clear the off-link flag, omit the off-link parameter when you issue this command. **Command mode**: Interface IP
ipv6 nd prefix *<IPv6 prefix> <IPv6 prefix length>* **valid-lifetime {***<0-4294967295>***|infinite|variable** *<0-4294967295>***} [prefered-lifetime {***<0-4294967295>***|infinite|variable}] [no-autoconfig] [off-link]** Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds. The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The default value is `2592000`. The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The default value is `604800`. **Note**: The Preferred Lifetime value must not exceed the Valid Lifetime value. **Command mode**: Interface IP
show ipv6 prefix *<IP interface number>* Displays current Neighbor Discovery prefix parameters. **Command mode**: All

IPv6 Prefix Policy Table Configuration

The following table describes the configuration options for the IPv6 Prefix Policy Table. The Prefix Policy Table allows you to override the default address selection criteria.

Table 346. *IPv6 Prefix Policy Table Options*

Command Syntax and Usage
`[no] ip prefix-policy` *<IPv6 prefix> <IPv6 prefix length> <precedence (0-100)> <label (0-100)>* Adds or removes a Prefix Policy Table entry. Enter the following parameters: o IPv6 address prefix o Prefix length o **Precedence**: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence. o **Label**: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match. **Command mode**: Global configuration
`show ip prefix-policy` Displays the current Prefix Policy Table configuration. **Command mode**: All

IP Loopback Interface Configuration

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

Table 347. *IP Loopback Interface Configuration Options*

Command Syntax and Usage
interface loopback *<1-5>* Enter Interface loopback mode. **Command mode**: Global configuration
no interface loopback *<1-5>* Deletes the selected loopback interface. **Command mode**: Global configuration
[no] enable Enables or disables the loopback interface. **Command mode**: Interface loopback
ip address *<IP address>* **[***<subnet mask>***] [enable]** Defines the loopback interface IP address. You can also specify its subnet mask. The `enable` option also enables the loopback interface. **Command mode**: Interface loopback
ip netmask *<subnet mask>* Defines the loopback interface subnet mask. **Command mode**: Interface loopback
ip ospf area *<0-19>* Configures the OSPF area index used by the loopback interface. **Command mode**: Interface loopback
[no] ip ospf enable Enables or disables OSPF for the loopback interface. **Command mode**: Interface loopback
no ip ospf Deletes the OSPF interface. **Command mode:** Interface loopback
show interface loopback *<1-5>* Displays the current IP loopback interface parameters. **Command mode**: All

DHCP Snooping

DHCP Snooping provides security by filtering untrusted DHCP packets and by maintaining a binding table of trusted interfaces.

Table 348. *DHCP Snooping Options*

Command Syntax and Usage
[no] ip dhcp snooping Enables or disables DHCP Snooping. **Command mode**: Global configuration
ip dhcp snooping binding *<MAC address>* **vlan** *<VLAN ID (1-4094)>* *<IP address>* **port** *<port alias or number>* **expiry** *<1-4294967295>* Adds a manual entry to the binding table. **Command mode**: Global configuration
no ip dhcp snooping binding {*<MAC address>***|all [interface port** *<port alias or number>***|vlan** *<VLAN ID (1-4094)>***]}** Removes an entry from the binding table. **Command mode**: Global configuration
[no] ip dhcp snooping information option-insert Enables or disables option 82 support for DHCP Snooping. When enabled, DHCP Snooping performs the following functions: o if a DHCP packet from a client contains option 82 information, the information is retained. o when DHCP Snooping forwards a DHCP packet from a client, option 82 information is added to the packet. owhen DHCP snooping forward a DHCP packet from a server, option 82 information is removed from the packet. **Command mode**: Global configuration
[no] ip dhcp snooping vlan *<VLAN ID (1-4094)>* Adds or removes the selected VLAN to DHCP Snooping. Member ports participate in DHCP Snooping. **Command mode**: Global configuration
show ip dhcp snooping Displays the current DHCP Snooping parameters. **Command mode**: All

Converged Enhanced Ethernet Configuration

The following table describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 349. *CEE Configuration Options*

Command Syntax and Usage
`[no] cee enable` Globally enables or disables CEE. **Command mode**: Global configuration
`[no] cee iscsi enable` Enables or disables ISCSI TLV advertisements. **Command mode**: Global configuration
`show cee iscsi` Displays the current ISCSI TLV parameters. **Command mode**: All
`show cee` Displays the current CEE parameters. **Command mode**: All

ETS Global Configuration

Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different traffic types, based on 802.1p priority.

Note: ETS configuration supersedes the QoS 802.1p menu and commands. When ETS is enabled, you cannot configure the 802.1p options.

ETS Global Priority Group Configuration

The following table describes the global ETS Priority Group configuration options.

Table 350. *Global ETS Priority Group Options*

Command Syntax and Usage
cee global ets priority-group pgid *<0-7, 15>* **bandwidth** *<bandwidth percentage (0, 10-100)>* Allows you to configure the link bandwidth percentage allocated to the Priority Group. **Note:** Priority Group 15 is a strict priority group and does not need bandwidth assigned to it. **Command mode**: Global configuration
cee global ets priority-group pgid *<0-7, 15>* **description** *<1-31 characters>* Enter text that describes this Priority Group. **Command mode**: Global configuration
no cee global ets priority-group *<0-7, 15>* **description** Deletes the Priority Group description. **Command mode:** Global configuration
cee global ets priority-group pgid *<0-7, 15>* **priority** *<802.1p priority (0-7)>* Allows you to assign one or more 802.1p values to the Priority Group. **Command mode**: Global configuration
show cee global ets Displays the current global ETS parameters. **Command mode**: All
show cee global ets priority-group *<0-7, 15>* Displays the current global ETS Priority Group parameters. **Command mode**: All

Priority Flow Control Configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

Global Priority Flow Control Configuration

Table 351 describes the global PFC Priority Group configuration options.

Table 351. *Global PFC Prority Group Commands*

Command Syntax and Usage
`[no] cee global pfc enable` Globally enables or disables Priority Flow Control on all ports. **Command mode:** Global configuration
`cee global pfc priority` *<0-7>* **`description`** *<1-31 characters>* Enter text that describes this Priority Group. **Command mode:** Global configuration
`no cee global pfc priority` *<0-7>* **`description`** Removes the description for the specified Priority Group. **Command mode:** Global configuration
`[no] cee global pfc priority` *<0-7>* **`enable`** Enables or disables Priority Flow Control for the specified priority level. **Command mode:** Global configuration
`show cee global pfc` Displays the current Priority Flow Control global configuration. **Command mode:** All

802.1p PFC Configuration

The following table describes the 802.1p Priority Flow Control (PFC) configuration options.

Table 352. *PFC 802.1p Configuration Options*

Command Syntax and Usage
[no] cee port *<port alias or number>* **pfc enable** Enables or disables Priority Flow Control on the specified port. **Command mode:** Global configuration
[no] cee port *<port alias or number>* **pfc priority** *<0-7>* **enable** Enables or disables Priority Flow Control on the selected 802.1p priority. **Note**: PFC can be enabled on 802.1p priority 3 and one other priority only. **Command mode**: Global configuration
cee port *<port alias or number>* **pfc priority** *<0-7>* **description** *<1-31 characters>* Enter text to describe the priority value. **Command mode**: Global configuration
no cee port *<port alias or number>* **pfc priority** *<0-7>* **description** Deletes the description for the specified priority value. **Command mode:** Global configuration
show cee port *<port alias or number>* **pfc** Displays the current 802.1p Priority Flow Control configuration on the specified port or ports. **Command mode**: All
show cee port *<port alias or number>* **pfc priority** *<0-7>* Displays the current 802.1p Priority Flow Control parameters. **Command mode**: All

DCBX Port Configuration

The following table describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 353. *Port DCBX Configuration Options*

Command Syntax and Usage
[no] cee port *<port alias or number>* **dcbx app_proto advertise** Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx app_proto willing** Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx enable** Enables or disables DCBX on the port. **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx ets advertise** Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx ets willing** Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx pfc advertise** Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
[no] cee port *<port alias or number>* **dcbx pfc willing** Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
show cee port *<port alias or number>* **dcbx** Displays the current port DCBX parameters. **Command mode**: All

FCoE Initialization Protocol Snooping Configuration

Fibre Channel over Ethernet (FCoE) transports Fibre Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

The following table describes the FCoE configuration options.

Table 354. *FCoE Configuration Options*

Command Syntax and Usage
`[no] fcoe fips automatic-vlan` Enables or disables automatic VLAN creation, based on response received from the connected device. **Command mode**: Global configuration
`[no] fcoe fips enable` Globally enables or disables FIP Snooping. **Command mode**: Global configuration
`[no] fcoe fips timeout-acl` Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system. **Command mode**: Global configuration
`show fcoe information` Displays the current FCoE parameters. **Command mode**: All

FIPS Port Configuration

FIP Snooping allows the switch to monitor FCoE Initialization Protocol (FIP) frames to gather discovery, initialization, and maintenance data. This data is used to automatically configure ACLs that provide FCoE connections and data security.

The following table describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 355. *Port FIP Snooping Options*

Command Syntax and Usage
`[no] fcoe fips port` *<port alias or number>* **`enable`** Enables or disables FIP Snooping on the port. The default setting is `enabled`. **Command mode**: Global configuration
`fcoe fips port` *<port alias or number>* **`fcf-mode [auto|on|off]`** Configures FCoE Forwarding (FCF) on the port, as follows: o `on`: Configures the port as a Fibre Channel Forwarding (FCF) port. o `off`: Configures the port as an FCoE node (ENode port). o `auto`: Automatically detect the configuration of the connected device, and configure this port to match. **Command mode**: Global configuration

Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 2819.

The following sections describe the Remote Monitoring (RMON) configuration options.

RMON History Configuration

The following table describes the RMON History commands.

Table 356. *RMON History Configuration Options*

Command Syntax and Usage
`rmon history` *<1-65535>* **`interface-oid`** *<1-127 characters>* Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: `1.3.6.1.2.1.2.2.1.1.X`, where `X` is the `ifIndex`. **Command mode**: Global configuration
`rmon history` *<1-65535>* **`owner`** *<1-127 characters>* Enter a text string that identifies the person or entity that uses this History index. **Command mode**: Global configuration
`no rmon history` *<1-65535>* **`owner`** Deletes the identification information for the specified History index. **Command mode:** Global configuration
`rmon history` *<1-65535>* **`polling-interval`** *<1-3600>* Configures the time interval over which the data is sampled for each bucket. The default value is `1800`. **Command mode**: Global configuration
`rmon history` *<1-65535>* **`requested-buckets`** *<1-65535>* Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is `30`. The maximum number of buckets that can be granted is 50. **Command mode**: Global configuration

Table 356. *RMON History Configuration Options*

Command Syntax and Usage
no rmon history *<1-65535>* Deletes the selected History index. **Command mode**: Global configuration
show rmon history Displays the current RMON History parameters. **Command mode**: All

RMON Event Configuration

The following table describes the RMON Event commands.

Table 357. *RMON Event Configuration Options*

Command Syntax and Usage
rmon event *<1-65535>* **description** *<1-127 characters>* Enter a text string to describe the event. **Command mode**: Global configuration
no rmon event *<1-65535>* **description** Deletes the description of the specified event index. **Command mode:** Global configuration
rmon event *<1-65535>* **owner** *<1-127 characters>* Enter a text string that identifies the person or entity that uses this Event index. **Command mode**: Global configuration
no rmon event *<1-65535>* **owner** Deletes the identification information for the specified Event index. **Command mode:** Global configuration
rmon event *<1-65535>* **type {log|trap|both}** Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. **Command mode**: Global configuration
no rmon event *<1-65535>* **type** Removes notification provided for this event. **Command mode:** Global configuration

Table 357. *RMON Event Configuration Options*

Command Syntax and Usage
no rmon event *<1-65535>* Deletes the selected RMON Event index. **Command mode**: Global configuration
show rmon event Displays the current RMON Event parameters. **Command mode**: All

RMON Alarm Configuration

The alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

The following table describes the RMON alarm commands.

Table 358. *RMON Alarm Configuration Options*

Command Syntax and Usage
rmon alarm *<1-65535>* **alarm-type {rising|falling|either}** Configures the alarm type as rising, falling or either (rising or falling). **Command mode**: Global configuration
rmon alarm *<1-65535>* **falling-crossing-index** *<0-65535>* Configures the falling alarm event index that is triggered when a falling threshold is crossed. **Command mode**: Global configuration
rmon alarm *<1-65535>* **falling-limit** *<-2147483647 - 2147483647>* Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. **Command mode**: Global configuration
rmon alarm *<1-65535>* **interval** *<1-65535>* Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is `1800`. **Command mode**: Global configuration
rmon alarm *<1-65535>* **oid** *<1-127 characters>* Configures an alarm MIB Object Identifier. **Command mode**: Global configuration

Table 358. *RMON Alarm Configuration Options (continued)*

Command Syntax and Usage
rmon alarm *<1-65535>* **owner** *<1-127 characters>* Enter a text string that identifies the person or entity that uses this alarm index. **Command mode**: Global configuration
no rmon alarm *<1-65535>* **owner** Deletes the identification information for the specified Alarm index. **Command mode:** Global configuration
rmon alarm *<1-65535>* **rising-crossing-index** *<0-65535>* Configures the rising alarm event index that is triggered when a rising threshold is crossed. **Command mode**: Global configuration
rmon alarm *<1-65535>* **rising-limit** *<-2147483647 - 2147483647>* Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. **Command mode**: Global configuration
rmon alarm *<1-65535>* **sample {abs|delta}** Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: o `abs` - absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. o `delta` - delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. **Command mode**: Global configuration
no rmon alarm *<1-65535>* Deletes the selected RMON Alarm index. **Command mode**: Global configuration
show rmon alarm Displays the current RMON Alarm parameters. **Command mode**: All

VMReady Configuration

The following table describes the VMReady configuration options.

Table 359. *VMReady Configuration Options*

Command Syntax and Usage
`[no] virt enable` Enables or disables VMReady. Before you enable VMReady, you must define one or more server ports. See "Server Port Configuration" on page 404. **Note**: The `no` form of this command deletes all configured VM groups. **Command mode**: Global configuration
`show virt` Displays the current virtualization parameters. **Command mode**: All

VM Policy Bandwidth Management

The following table describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 360. *VM Bandwidth Management Options*

Command Syntax and Usage
`[no] virt vmpolicy vmbwidth {`*<MAC address>***`|`***<UUID>***`|`***<name>***`| |`***<IP address>***`|`***<index number>***`} bwctrl`** Enables or disables bandwidth control on the VM policy. **Command mode:** Global configuration
`virt vmpolicy vmbwidth {`*<MAC address>***`|`***<UUID>***`|`***<name>***`| |`***<IP address>***`|`***<index number>***`} rxrate`** *<0-40000000> <max. burst (0-4096)>* The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: `0`, `32`, `64`, `128`, `256`, `512`, `1024`, `2048` or `4096`. **Command mode:** Global configuration

Table 360. *VM Bandwidth Management Options (continued)*

Command Syntax and Usage
virt vmpolicy vmbwidth {<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**} txrate** <*0-40000000*> <*max. burst (0-4096)*> **[**<*ACL number*>**]** The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: `0`, `32`, `64`, `128`, `256`, `512`, `1024`, `2048` or `4096`. The third value represents the ACL assigned to the transmission rate. The ACL is added automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one. **Command mode:** Global configuration
no virt vmpolicy vmbwidth {<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**}** Deletes the bandwidth management settings from this VM policy. **Command mode:** Global configuration
show virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**|**<*index range*>**] [|{include|exclude|** **|section|begin}]** Displays the current VM bandwidth management parameters for all virtual machines or only for a certain VM by specifying its MAC address, UUID, name, IP address or index number. o `|` displays the VM bandwidth management parameters matching one of the following filters: • `include` displays parameters matching the specified expression • `exclude` displays parameters not matching the specified expression • `section` displays parameters matching the specified section • `begin` displays parameters beginning from the first parameter that matches the specified expression **Command mode:** All

VM Group Configuration

The following table describes the VM group configuration options. A VM group is a collection of members, such as VMs, ports or Link Aggregation Groups (LAGs). Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 361. *VM Group Configuration Options*

Command Syntax and Usage
[no] virt vmgroup *<1-4096>* **cpu** Enables or disables sending unregistered IPMC traffic to the CPU. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **flood** Enables or disables the flooding of unregistered IPMC traffic. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **key** *<1-65535>* Adds or removes an LACP *admin key* to/from the VM group. LACP LAGs formed with this *admin key* will be included in the VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **optflood** Enables or disables Optimized Flooding on the VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **port** *<port alias or number>* Adds or removes the selected port to/from the VM group. **Note**: A port can be added to a VM group only if no VMs on that port are members of the VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **portchannel** *<1-72>* Adds or removes the selected LAG to/from the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **profile** *<profile name (1-39 characters)>* Adds the selected VM profile to the VM group. **Note:** This command can only be used if the VM group is empty (that is, it only has a profile assigned). **Command mode:** Global configuration
no virt vmgroup *<1-4096>* **profile** Removes the VM profile assigned to the VM group. **Note:** This command can only be used if the VM group is empty (only has the profile assigned). **Command mode:** Global configuration

Table 361. *VM Group Configuration Options (continued)*

Command Syntax and Usage
virt vmgroup *<1-4096>* **stg** *<1-128>* Assigns the VM group to a Spanning Tree Group (STG). **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **tag** Enables or disables VLAN tagging on ports in this VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **validate {basic|advanced}** Enables MAC address spoof prevention for the specified VM group. o `basic` validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for "trusted" hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines. o `advanced` validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for "untrusted" hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines. The default setting is `disabled`. **Command mode:** Global configuration
no virt vmgroup *<1-4096>* **validate** Disables MAC address spoof prevention for the specified VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **vlan** *<VLAN ID (1-4094)>* Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns the first unused VLAN when adding a port or a VM to the VM Group. **Note**: If you add a VM profile to this group, the group will use the VLAN assigned to the profile. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **vm {***<VM MAC address index (0-4095)>***||***<MAC address>***|***<UUID>***|***<name>***|***<IP address>***}** Adds or removes a VM to/from the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (`virt vmware vcspec`). The VM index number is found in the VM information dump (`show virt vm`). **Note**: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group. **Command mode:** Global configuration

Table 361. *VM Group Configuration Options (continued)*

Command Syntax and Usage
`[no] virt vmgroup` *<1-4096>* **`vmap`** *<1-128>* **`[serverports| |non-serverports]`** Adds or removes the selected VLAN Map to/from this group. You can choose to limit operation of the VLAN Map to server ports only or non-server ports only. If you do not select a port type, the VMAP is applied to the entire VM Group. For more information about configuring VLAN Maps, see "VMAP Configuration" on page 448. **Command mode:** Global configuration
`[no] virt vmgroup` *<1-4096>* **`vport`** *<1-8>* Adds or removes the selected virtual port to the VM group. **Command mode:** Global configuration
`no virt vmgroup` *<1-4096>* Deletes the VM group. **Command mode:** Global configuration
`show virt vmgroup` *<1-4096>* Displays the current VM group parameters. **Command mode:** All

VM Check Configuration

The following table describes the VM Check validation options used for MAC address spoof prevention.

Table 362. *VM Check Configuration Options*

Command Syntax and Usage
`virt vmcheck acls max` *<1-256>* Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. The default value is `50`. **Command mode:** Global configuration
`default virt vmcheck acls` Sets to default maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. **Command mode:** Global configuration
`no virt vmcheck acls` Disables ACL-based MAC address spoofing prevention in advanced validation mode. **Command mode:** Global configuration
`virt vmcheck action advanced {acl|link|log}` Sets up action taken when detecting MAC address spoofing in advanced validation mode: o `acl` registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address o `link` registers a syslog entry and disables the corresponding switch port o `log` registers a syslog entry The default setting is `acl`. **Command mode:** Global configuration
`virt vmcheck action basic {link|log}` Sets up action taken when detecting MAC address spoofing in basic validation mode: o `link` registers a syslog entry and disables the corresponding switch port o `log` registers a syslog entry The default setting is `link`. **Command mode:** Global configuration
`default virt vmcheck action {advanced|basic}` Sets to default action taken when detecting MAC address spoofing in advanced or basic validation mode. **Command mode:** Global configuration

Table 362. *VM Check Configuration Options*

Command Syntax and Usage
`[no] virt vmcheck trust` *<port alias or number>* Enables or disables trusted ports for VM communication. By default, all ports are `disabled`. **Command mode:** Global configuration
`show virt vmcheck` Displays the current VM Check settings. See page 171 for sample output. **Command mode**: All

VM Profile Configuration

The following table describes the VM Profiles configuration options.

Table 363. *VM Profile Configuration Options*

Command Syntax and Usage
`virt vmprofile` *<profile name (1-39 characters)>* Defines a name for the VM profile. The switch supports up to 2048 VM profiles. **Command mode:** Global configuration
`no virt vmprofile` *<profile name (1-39 characters)>* Deletes the selected VM profile. **Command mode:** Global configuration
`virt vmprofile edit` *<profile name (1-39 characters)>* **`eshaping`** *<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>* Configures traffic egress shaping parameters implemented in the hypervisor, as follows: o Average traffic, in kilobits per second. o Maximum burst size, in kilobits. o Peak traffic, in kilobits per second. o Delete traffic shaping parameters. **Command mode:** Global configuration
`no virt vmprofile` *<profile name (1-39 characters)>* **`eshaping`** Deletes the traffic egress shaping parameters for the specified VM profile. **Command mode:** Global configuration

Table 363. *VM Profile Configuration Options*

Command Syntax and Usage
virt vmprofile edit *<profile name (1-39 characters)>* **shaping** *<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>* Configures traffic shaping parameters implemented in the hypervisor, as follows: o Average traffic, in kilobits per second. o Maximum burst size, in kilobits. o Peak traffic, in kilobits per second. o Delete traffic shaping parameters. **Command mode:** Global configuration
no virt vmprofile *<profile name (1-39 characters)>* **shaping** Deletes the traffic shaping parameters for the specified VM profile. **Command mode:** Global configuration
virt vmprofile edit *<profile name (1-39 characters)>* **vlan** *<VLAN ID (1-4094)>* Assigns a VLAN to the VM profile. **Command mode:** Global configuration
show virt vmprofile [*<profile name>***]** Displays the current VM Profile parameters. **Command mode:** All

VMWare Configuration

The following table describes the VMware configuration options. When you configure the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

Table 364. *VM Ware Configuration Options*

Command Syntax and Usage
virt vmware hbport *<1-65535>* Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port `902`. **Command mode:** Global configuration
default virt vmware hbport Sets to default esx/esxi server to vcenter heartbeat udp port. **Command mode**: Global configuration
virt vmware hello {enable|haddr *<IP address>***|hport** *<port alias or number>***|htimer** *<1-60>***}** Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention. Default setting is disabled. o `enable` enables CDP advertisements transmission. o `haddr` advertises a specific IP address instead of the default `0.0.0.0` IP. o `hport` enables ports on which CDP advertisements are sent. o `htimer` sets the number of seconds between successive CDP advertisements. The default value is `30` seconds. **Command mode:** Global configuration
default virt vmware hello htimer Sets to default HELLO periodicity. **Command mode**: Global configuration
no virt vmware hello {enable|hport *<port alias or number>***}** Disables CDP advertisement transmissions completely or only on specific ports. **Command mode**: Global configuration

Table 364. *VM Ware Configuration Options*

Command Syntax and Usage
virt vmware vcspec *<IP address> <username>* **[noauth]** Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system. You are prompted for the following information: o IP address of the Virtual Center o User name and password for the Virtual Center o Whether to authenticate the SSL security certificate (yes or no) **Command mode:** Global configuration
no virt vmware vcspec Deletes the Virtual Center credentials on the switch. **Command mode:** Global configuration
show virt vmware Displays the current VMware parameters. **Command mode:** All

Miscellaneous VMReady Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the Enterprise NOS CLI and the Miscellaneous VMReady Configuration Menu. The following table describes the VMReady configuration options.

Table 365. *VMReady Configuration Options*

Command Syntax and Usage
[no] virt vmrmisc lmac Enables or disables the switch to treat locally administered MAC addresses as VMs. **Command mode:** Global configuration
virt vmrmisc oui *<3 byte VM MAC OUI> <Vendor Name>* Adds a MAC OUI. **Command mode:** Global configuration
no virt vmrmisc oui *<3 byte VM MAC OUI>* Removes a MAC OUI. **Command mode:** Global configuration
show virt oui Displays all the configured MAC OUIs. **Command mode:** All

UFP Configuration

The following table describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 8 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, auto, or FCoE) and within predefined bandwidth limits.

Table 366. *UFP Commands*

Command Syntax and Usage
[no] ufp enable Globally enables or disables UFP. **Command mode:** Global configuration
[no] ufp port *<port number>* **enable** Enables or disables UFP on the specified physical port. **Command mode:** Global configuration
ufp port *<port number>* **qos-mode {bw|ets}** Configures the Quality of Service (QoS) mode for the specified UFP port. o `bw` - performs rate bandwidth control by dividing the port's bandwidth across the virtual ports. A minimum and a maximum limit can be configured for each virtual port. **Note**: QoS Bandwidth mode is only applicable to up to four virtual ports per physical port. o `ets` - Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different virtual ports, based on 802.1q priority. **Note**: QoS ETS mode requires Converged Enhanced Ethernet (CEE) to enabled on the switch. For details, see page 629. The default setting is `bw`. **Command mode**: Global configuration
ufp port *<port number>* **vport** *<1-8>* Enters UFP Virtual Port Configuration mode. **Command mode:** Global configuration
no ufp port *<port number>* **[vport** *<1-8>***]** Removes UFP settings from the specified physical or virtual port. **Command mode:** Global configuration
[no] enable Enables or disables the virtual port. **Command mode:** UFP Virtual Port Configuration
evb profile *<1-16>* Applies the specified EVB profile for the virtual port. **Command mode:** UFP Virtual Port Configuration

Table 366. *UFP Commands (continued)*

Command Syntax and Usage
no evb profile Resets the EVB profile for the virtual port. **Command mode:** UFP Virtual Port Configuration
network {mode [access|trunk|tunnel|auto|fcoe]|default-vlan *<VLAN ID (2-4094)>***|default-tag}** Configures the virtual port network configuration settings: o `mode` configures the virtual port's operating mode: • `access` allows the virtual port to associate only with the default customer VLAN, as defined by the default-vlan option. • `trunk` allows the virtual port to associate with up to 1024 customer VLANs depending on the number of virtual ports enabled on the UFP port. • `tunnel` makes the virtual port VLAN agnostic. • `auto` allows the virtual port to be dynamically associated with VLANs through VMready or QBG. • `fcoe` configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. CEE/FCoE should be enabled globally and priority 3 configured for the virtual port before enabling an FCoE virtual port. o `default-vlan` configures the default VLAN ID for the virtual port. This option provides an override if conflicts arise with a customer VLAN ID on the upstream network. o `default-tag` enables tagging egress frames with the default VLAN ID when the virtual port is in trunk mode and `default-vlan` is defined. The default setting is `disabled`. **Note:** VLANs 4002-4009 cannot be used as customer VLANs. **Note:** A customer VLAN cannot be configured on multiple virtual ports of the same physical port. **Command mode:** UFP Virtual Port Configuration
no network default-tag Disables default VLAN ID tagging on the virtual port. **Command mode:** UFP Virtual Port Configuration

Table 366. *UFP Commands (continued)*

Command Syntax and Usage
network private-vlan {host|trunk|promiscuous} Configures the virtual port's Private VLAN mode: o `host` allows only ONE secondary VLAN. In case of network trunk mode, the other VLANs will be in non-Private VLANs. A virtual port operating in Private VLAN host mode cannot belong to multiple Private VLAN domains. o `trunk` allows both primary and secondary VLAN as well as non-Private VLAN domains. The Isolate-VLAN is also allowed to pass through this port type. o `promiscuous` allows private VLAN promiscuous mode **Note:** Virtual ports that are part of the same physical port cannot belong to the same Private VLAN domain. **Command mode:** UFP Virtual Port Configuration
no network private-vlan Disables private-VLAN mode on the virtual port. **Command mode:** UFP Virtual Port Configuration
qos bandwidth {max *<10-100>*|**min** *<10-100>***}** Configures bandwidth allocation for the virtual port: o Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is `25`. o Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is `100`. **Note**: The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100. **Command mode:** UFP Virtual Port Configuration
qos ets priority *<802.1q priority(0-7)>* Configures the 802.1q priority of the traffic going through the virtual port. The default value is `0`. **Command mode**: UFP Virtual Port Configuration
[no] qos ets host-control Enables or disables the switch to automatically configure the 802.1p priority of the traffic traversing the virtual port. The default value is `disabled`. **Command mode**: UFP Virtual Port Configuration

Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). The following table describes EVB configuration commands.

Table 367. *Edge Virtual Bridge Configuration Options*

Command Syntax and Usage
virt evb vsidb *<VSIDB number>* Enter Virtual Station Interface Database configuration mode. For more details, see page 654. **Command mode:** Global configuration
virt evb profile *<profile number>* Enter Virtual Station Interface Profile configuration mode. For more details, see page 656. **Command mode:** Global configuration
show virt evb vsidb *<VSIDB number>* Displays the current Virtual Station Interface database information. **Command mode:** All
show virt evb profile [*<profile number>***]** Displays the current EVB profile parameters. **Command mode:** All

Edge Virtual Bridge VSI Type Database Configuration

The following table describes the EVB VSI Type Database configuration options.

Table 368. *Edge Virtual Bridge VSI Type Database Configuration Options*

Command Syntax and Usage
virt evb vsidb *<VSIDB number>* Enter Virtual Station Interface Database configuration mode. **Command mode:** Global configuration
filename *<file name>* Sets the Virtual Station Interface Type database document name. **Command mode:** VSI Database
no filename Deletes the Virtual Station Interface Type database document name. **Command mode:** VSI Database
filepath *<file path>* Sets the Virtual Station Interface Type database document path. **Command mode:** VSI Database
no filepath Deletes the Virtual Station Interface Type database document path. **Command mode:** VSI Database
host *<IP address>* **[mgt-port|data-port]** Sets the Virtual Station Interface Type database manager IP address and the port used for the connection. By default, the management port is used. **Command mode:** VSI Database
port *<1-65534>* Sets the Virtual Station Interface Type database manager port. **Command mode:** VSI Database
protocol {http|https} Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP. **Command mode:** VSI Database
update-interval *<5-300>* Sets the Virtual Station Interface Type database update interval in seconds. **Command mode:** VSI Database
[no] update-interval Disables the Virtual Station Interface Type database periodic update. **Command mode:** VSI Database

Table 368. *Edge Virtual Bridge VSI Type Database Configuration Options (continued)*

Command Syntax and Usage
no virt evb vsidb *<VSIDB number>* Resets the Virtual Station Interface Type database information to the default values. **Command mode:** Global configuration
show virt evb vsitypes [mgrid *<0-255>***|typeid** *<1-16777215>***| |version** *<0-255>***]** Displays the current Virtual Station Interface Type database parameters. **Command mode:** All
show virt evb vsidb *<VSIDB number>* Displays the current Virtual Station Interface database information. **Command mode:** All

Edge Virtual Bridge VSI Type Profile Configuration

The following table describes the Virtual Station Interface Type profile configuration options.

Table 369. *Edge Virtual Bridge VSI Type Profile Configuration Options*

Command Syntax and Usage
virt evb profile *<profile number>* Enter Virtual Station Interface type profile configuration mode. **Command mode:** Global configuration
[no] reflective-relay Enables or disables VEPA mode (Reflective Relay capability). **Command mode:** EVB Profile
[no] vsi-discovery Enables or disables VSI Discovery (ECP and VDP). **Command mode:** EVB Profile
no virt evb profile *<profile number>* Deletes the specified EVB profile. **Command mode:** Global configuration
evb profile *<1-16>* Applies the specified EVB profile for the port. Automatically enables LLDP EVB TLV on the corresponding port. **Command mode:** Interface port
no evb profile Resets EVB profile for the port. Automatically disables LLDP EVB TLV on the corresponding port. **Command mode:** Interface port
show virt evb profile [*<1-16>***]** Displays the current EVB profile parameters. **Command mode:** All
show virt evb profile ports Displays all EVB profile parameters including ports. **Command mode:** All

Networking Virtualization Configuration

The following table describes the Networking Virtualization (NWV) configuration options.

Table 370. *Networking Virtualization Configuration Options*

Command Syntax and Usage
nwv mode nsx-gw Enables the VXLAN Gateway. The default settings is `disabled`. **Command mode:** Global configuration
no nwv mode Disables the VXLAN Gateway. **Command mode:** Global configuration
[no] nsx-gw enable Enables or disables the VXLAN Gateway on the switch port. **Command mode**: Interface port
nwv nsx-gw Enters the VXLAN Gateway configuration mode. **Command mode:** Global configuration
controller ip *<IPv4 address>* **[data-port|mgt-port]** Configures the NSX controller IP address. **Configuration mode:** VXLAN Gateway
controller port *<TCP port (1-65534)>* Configures the NSX controller port. **Configuration mode:** VXLAN Gateway
no controller Removes the NSX controller configuration. **Configuration mode:** VXLAN Gateway
tunnel ip *<IPv4 address>* Configures the VXLAN Gateway tunnel IP address. **Command mode:** VXLAN Gateway
no tunnel Removes the VXLAN Gateway tunnel configuration. **Command mode:** VXLAN Gateway
show nwv nsx-gw Displays VXLAN Gateway information. For a sample output, see page 181. **Command mode:** All

OpenFlow Configuration

OpenFlow is an open interface used to control the forwarding plane in compatible switches and routers remotely, from an external controller. The RackSwitch G8272 can function as either a Hybrid or OpenFlow-only switch:

- In Hybrid mode (default), an OpenFlow pipeline can be set up to run in parallel to the normal Ethernet switching pipeline. The two pipelines are completely separate, each with its own dedicated ports and confined packet flows.
- In OpenFlow-only mode, the normal Ethernet switching capabilities are disabled, and the RackSwitch G8272 behaves as a pure OpenFlow switch.

The following table describes the OpenFlow configuration options.

Table 371. *OpenFlow Configuration Options*

Command Syntax and Usage
boot openflow {v1|v13} Switches between OpenFlow version 1.0 and OpenFlow version 1.3 on reboot. The default setting is `v1`. **Command mode:** Global configuration
boot profile default Starts the switch in Hybrid mode on reboot. This is the default setting. **Command mode:** Global configuration
boot profile openflow Starts the switch in OpenFlow-only mode on reboot. **Command mode:** Global configuration
[no] openflow enable Enables or disables OpenFlow. **Note:** Features involving TCAM resources are not supported on all ports. **Command mode:** Global configuration
openflow fdb-priority *<1-65535>* Configures a priority value to map flows with matching priority to FDB entries, if the flow uses destination MAC address and VLAN as the matching qualifier and single port as the action. The default value is `1000`. **Note**: When you issue this command, all registered flow entries are cleared. **Command mode**: Global configuration
no openflow fdb-priority Resets priority value required for FDB flows to the default value of `1000`. **Command mode:** Global configuration

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
`openflow fdb-timeout` *<1-300>* Configures a time interval in seconds for periodically clearing dynamically learned FDB entries on edge ports. The default value is `disabled`. **Command mode**: Global configuration
`no openflow fdb-timeout` Disables periodical clearing of dynamically learned FDB entries on edge ports. **Command mode**: Global configuration
`[no] openflow mgmtport` *<port alias or number>* Enables or disables OpenFlow management for the selected port. Use OpenFlow management ports to communicate with an OpenFlow Controller. In Hybrid mode, controllers can also connect to the switch using legacy ports. **Note:** Supported only in OpenFlow Only mode. The default setting is `disabled`. **Command mode**: Global configuration
`openflow mpls-priority` *<1-65535>* Configures a priority value to map flows with matching priority to MPLS entries. The default value is `65535`. **Note**: Supported only in OpenFlow 1.3. **Note**: When you issue this command, all the existing MPLS flows are cleared automatically. **Command mode**: Global configuration
`no openflow mpls-priority` Resets the priority value required for MPLS flows to the default value of `65535`. **Note**: Supported only in OpenFlow 1.3. **Command mode:** Global configuration
`openflow instance` *<1-2>* Enters OpenFlow Instance command mode for the specified instance ID. **Command mode**: Global configuration
`no openflow instance` *<1-2>* Deletes the instance and clears flow table and statistics for the specified instance ID. **Command mode:** Global configuration

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
[no] buffer Enables or disables buffering support for OpenFlow packets. The default setting is `disabled`. **Command mode**: OpenFlow Instance
connect-retry *<1-8>* Configures the maximum number of attempts to establish connection to a controller, before assuming the controller is down. The default value is `4`. **Command mode**: OpenFlow Instance
no connect-retry Resets the `connect-retry` value to 4. **Command mode**: OpenFlow Instance
controller *<1-4>* **address** *<IP address>* **[data-port|mgt-port]** Configures the IP address of the OpenFlow Controller. You may specify the port to use for data transfer: data port (`data-port`) or management port (`mgt-port`). By default, the system uses the management port. **Command mode:** OpenFlow Instance
controller *<1-4>* **port** *<TCP port number (1-65535)>* Configures the TCP port used for communication with the Controller. The default port is `6633`. **Command mode:** OpenFlow Instance
no controller *<1-4>* Deletes the selected controller from the specified instance ID. **Command mode**: OpenFlow Instance
dpid *<hex string>* Applies an 8 byte Datapath ID to the instance, which uniquely identifies an OpenFlow instance in an OpenFlow environment. The default value is the instance ID followed by the switch MAC. **Note:** The Datapath ID must be unique among the switches controlled by a single OpenFlow controller. **Command mode**: OpenFlow Instance
no dpid Resets the instance's Datapath ID to the default value (instance ID followed by the switch MAC). **Command mode**: OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
`echo-reply-timeout` *<2-65535>* Configures the duration in seconds the switch will wait to receive an echo reply from the controller, before assuming failure. The default value is `15` seconds. **Note:** The `echo-reply-timeout` value must be lower than the `echo-request-interval` value. **Command mode**: OpenFlow Instance
`no echo-reply-timeout` Resets the `echo-reply-timeout` to the default value of `15` seconds. **Command mode**: OpenFlow Instance
`echo-request-interval` *<5-65535>* Configures the maximum duration in seconds the switch will keep sending echo requests to a non-responsive controller. The default value is `30` seconds. **Note:** The `echo-request-interval` value must be higher than the `echo-reply-timeout` value. **Command mode**: OpenFlow Instance
`no echo-request-interval` Resets the `echo-request-interval` to the default value of `30` seconds. **Command mode**: OpenFlow Instance
`[no] edgeport` *<port alias or number>* Enables or disables the selected port as an OpenFlow edge port (outside port). Edge ports are usually connected to servers. The default setting is `disabled`. **Note**: Learning and flood blocking are turned on in OpenFlow edge ports. **Command mode**: OpenFlow Instance
`[no] edgeport portchannel` *<1-144>* Enables or disables the selected portchannel as an OpenFlow edge portchannel (outside portchannel). Edge portchannels are usually connected to servers. The default setting is `disabled`. **Note**: Learning and flood blocking are turned on in OpenFlow edge portchannels. **Note:** Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
emergency [timeout *<0-3600>***]** Forces the instance in emergency mode. The `timeout` parameter configures the duration in seconds after which the emergency mode expires. The default value is `30` seconds. **Note**: Supported only in OpenFlow 1.0. **Command mode**: OpenFlow Instance
no emergency [timeout] Brings the instance out of emergency mode. The `timeout` parameter resets the emergency mode duration to the default value of `30` seconds. **Note**: Supported only in OpenFlow 1.0. **Command mode:** OpenFlow Instance
[no] enable Enables or disables the instance. **Note:** When disabling an instance, its flow tables and statistics are cleared. **Command mode**: OpenFlow Instance
max-flow-acl *<0-1500>* **max-flow-acl** *<0-2000>* Enables or disables the maximum flow ACL option, which ensures a dedicated maximum number of ACL flows are available for the instance. The maximum number of entries is 1500 in Hybrid mode and 2000 in OpenFlow Only mode. The total number of 1500/2000 entries is shared between instances. By default, `max-flow-acl` is set to `0`, allowing instances to dynamically access the available ACL flow slots until depletion. **Note:** Setting `max-flow-acl` manually limits the number of ACL flow slots available for other instances by the corresponding value. **Command mode**: OpenFlow Instance
no max-flow-acl Sets the instance's maximum number of ACL based flows to the default value of `0` (dynamic allocation). **Command mode:** OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
max-flow-mcast-fdb *<0-4096>* Enables or disables the maximum flow multicast FDB option, which ensures a dedicated maximum number of FDB multicast flows are available for the instance. The total number of entries is shared between instances. By default, max-flow-mcast-fdb is set to 0, allowing instances to dynamically access the available FDB multicast flow slots until depletion. **Note:** Setting max-flow-mcast-fdb manually limits the number of FDB multicast flow slots available for other instances by the corresponding value. **Command mode:** OpenFlow Instance
no max-flow-mcast-fdb Sets the instance's maximum number of FDB based multicast flows to the default value of 0 (dynamic allocation). **Command mode:** OpenFlow Instance
max-flow-mpls-pop *<0-1000>* Enables or disables the maximum flow MPLS pop option, which ensures a dedicated maximum number of MPLS label pop flows are available for the instance. The total number of 1000 entries is shared between instances. By default, max-flow-mpls-pop is set to 0, allowing instances to dynamically access the available MPLS label pop flow slots until depletion. **Note:** Setting max-flow-mpls-pop manually limits the number of MPLS label pop flow slots available for other instances by the corresponding value. **Note**: Supported only in OpenFlow 1.3. **Command mode:** OpenFlow Instance
no max-flow-mpls-pop Sets the instance's maximum number of MPLS label pop flows to the default value of 0 (dynamic allocation). **Note**: Supported only in OpenFlow 1.3. **Command mode:** OpenFlow Instance
max-flow-mpls-push *<0-2000>* Enables or disables the maximum flow MPLS push option, which ensures a dedicated maximum number of MPLS label push flows are available for the instance. The total number of 2000 entries is shared between instances. By default, max-flow-mpls-push is set to 0, allowing instances to dynamically access the available MPLS label push flow slots until depletion. **Note:** Setting max-flow-mpls-push manually limits the number of MPLS label push flow slots available for other instances by the corresponding value. **Note**: Supported only in OpenFlow 1.3. **Command mode:** OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
no max-flow-mpls-push Sets the instance's maximum number of MPLS label push flows to the default value of `0` (dynamic allocation). **Note**: Supported only in OpenFlow 1.3. **Command mode:** OpenFlow Instance
max-flow-ucast-fdb *<0-123904>* Enables or disables the maximum flow unicast FDB option, which ensures a dedicated maximum number of FDB unicast flows available for the instance. The total number of entries is shared between instances. By default, `max-flow-ucast-fdb` is set to `0`, allowing instances to dynamically access the available FDB unicast flow slots until depletion. **Note:** Setting `max-flow-ucast-fdb` manually limits the number of FDB unicast flow slots available for other instances by the corresponding value. **Command mode:** OpenFlow Instance
no max-flow-ucast-fdb Sets the instance's maximum number of FDB based unicast flows to the default value of `0` (dynamic allocation). **Command mode:** OpenFlow Instance
[no] member *<port alias or number>* Enables or disables port usage by the OpenFlow instance for data traffic. **Command mode**: OpenFlow Instance
[no] member portchannel *<1-144>* Enables or disables static portchannel or LACP usage by the OpenFlow instance for data traffic. **Note**: Static portchannels and LACPs are supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
min-flow-timeout *<1-300>* Sets the minimum number of seconds after which a flow can be cleared from the instance's tables. The default value is `0`, meaning controller provided values are used instead. **Command mode**: OpenFlow Instance
no min-flow-timeout Sets the number of seconds after which a flow can be cleared from the instance's tables to the default value of `0` (controller provided values). **Command mode**: OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
mirror-to-controller cookie *<0x0-0xffffffffffffffff>* Sets the flow cookie for packets sent to controller as a result of a mirror-to-controller setting (flow is set to output the packet to a controller in addition to another destination). The default value is `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
no mirror-to-controller cookie Resets the mirror-to-controller flow cookie to the default value of `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
send-to-controller cookie *<0x0-0xffffffffffffffff>* Sets the flow cookie for packets sent to controller as a result of a send-to-controller setting (flow is set to output the packet only to a controller). The default value is `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
no send-to-controller cookie Resets the send-to-controller flow cookie to the default value of `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
static-table Configures static flows. For command options, see page 668. **Command mode:** OpenFlow Instance
table-miss cookie *<0x0-0xffffffffffffffff>* Sets the flow cookie for packets sent to controller as a result of a table-miss setting (send input packets that don't match any flow entries to controller). The default value is `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
no table-miss cookie Resets the table-miss flow cookie to the default value of `0xffffffffffffffff`. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
`[no] table-miss controller` Sets or disables the `table-miss` flow entry to send packets unmatched by any flow entries to the controller. The default value is `disabled`, meaning packets unmatched by flow entries are dropped. **Note**: Supported only in OpenFlow 1.3. **Command mode**: OpenFlow Instance
`[no] openflow fdb-aging` Enables or disables periodical clearing of dynamically learned FDB entries on a specific port. The default value is `disabled` on OpenFlow edge ports. **Command mode**: Interface port/Interface portchannel
`[no] openflow static-station-move` Enables or disables forwarding frames that have source MAC addresses conflicting with entries in the static FDB table. This enables equal cost multi-path routing and use cases where IPS and Firewall devices forward packets without changing the source MAC address. The default value is `disabled`. **Command mode**: Interface port/Interface portchannel
`clear openflow {group|table [basic|emergency|dynamic| |static]}` Clears OpenFlow data for all instances: o The `group` option clears the OpenFlow 1.3 group table. o The `table` option clears all basic and emergency OpenFlow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables. • The `basic` option clears only the basic OpenFlow tables. • The `emergency` option clears only the emergency OpenFlow tables. • The `dynamic` option clears only the dynamic OpenFlow tables. • The `static` option clears only the static OpenFlow tables. **Command mode:** Privileged EXEC

Table 371. *OpenFlow Configuration Options (continued)*

Command Syntax and Usage
`clear openflow instance` *<1-2>* **`{group|table [basic|emergency|dynamic|static]}`** Clears OpenFlow data for the specified instance ID: o The `group` option clears the OpenFlow 1.3 group table. o The `table` option clears all basic and emergency OpenFlow tables in OpenFlow 1.0. In OpenFlow 1.3, clears the dynamic and static flow tables. • The `basic` option clears only the basic OpenFlow table. • The `emergency` option clears only the emergency OpenFlow table. • The `dynamic` option clears only the emergency OpenFlow tables. • The `static` option clears only the static OpenFlow tables. **Command mode:** Privileged EXEC
`show openflow [flow-allocation|group|information|table]` Displays the current OpenFlow configuration. For more information, see page 150. o `flow-allocation` displays the configured, current and maximum number of flows for all OpenFlow instances. For more information, see page 152. o `group` displays group information for all OpenFlow 1.3 instances. For more information, see page 154. o `information` displays the configuration for all OpenFlow instances. For more information, see page 155. o `table` displays the basic and emergency flow tables for all OpenFlow instances in OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables. For more information, see page 157 **Command mode:** All
`show openflow instance` *<1-2>* **`[group|information|table]`** Displays OpenFlow information for the specified instance ID: o `group` displays group information per instance. o `information` displays the instance configuration. o `table` displays the basic and emergency flow tables per instancein OpenFlow 1.0. In OpenFlow 1.3, displays the dynamic and static flow tables per instance. **Command mode:** All

Static Flows Configuration

Static flows are ACL OpenFlow entries set up manually from the CLI by the administrator. Static flows cannot be deleted/modified by OpenFlow controllers and will continue to function when the switch goes into emergency mode. Even if they qualify as FDB entries based on their settings, static flows are always stored as ACL entries. A total of maximum 1000 static flows pool is shared between all OpenFlow instances.

The following table describes the static flow configuration options:

Table 372. *Static FlowsConfiguration Options*

Command Syntax and Usage
static-table add index *<1-1000>* **match** *<matching qualifier>* **actions** *<matching qualifier>* **[options** *<matching qualifier>***]** **priority** *<0-65535>* Adds a static flow entry to the instance. **Command mode:** OpenFlow Instance
static-table modify index *<1-1000>* **match** *<matching qualifier>* **actions** *<matching qualifier>* **[options** *<matching qualifier>***]** **priority** *<0-65535>* Overwrites a static flow entry. **Command mode:** OpenFlow Instance
static-table remove index *<1-1000>* Deletes a static flow entry. **Command mode:** OpenFlow Instance
clear openflow table static Deletes all static flow entries. **Command mode:** Privileged EXEC

The following table describes the available matching qualifiers:

Table 373. *Static Flow Matching Qualifiers in OpenFlow 1.0*

Qualifier	Value
ingress-port	Port of instance
src-mac	Source MAC address
dst-mac	Destination MAC address
vlan-id	VLAN identifier (0-4095 + 65535 (untagged))
vlan-priority	802.1p Priority Code Point (0-7)
src-ip	Source IP address
dst-ip	Destination IP address
src-port	L4 source port (0-65536)
dst-port	L4 destination port (0-65535)
ether-type	"arp"/"0806" or "ip"/"0800" or (hex-value <= 65535)
protocol	"tcp" or "udp" or 0-255
tos	IP Type of Service (0-255)
type	"request" or "reply" (can be set only if ether type is ARP)
all	Applicable to all traffic

Table 374. *Static Flow Matching Qualifiers in OpenFlow 1.3*

Qualifier	Value
in-port	switch input port
in-portchannel	switch input portchannel
in-phy-port	switch physical input port, valid only when in-port is specified
eth-src	source MAC address and mask
eth-dst	destination MAC address and mask
vlan-vid	VLAN identifier (0-4095 + 65535 (untagged))
vlan-pcp	802.1p(0-7)
ipv4-src	source IPv4 address and mask
ipv4-dst	destination IPv4 address and mask
tcp-src	TCP source port (0-65535)
tcp-dst	TCP destination port (0-65535)

Table 374. *Static Flow Matching Qualifiers in OpenFlow 1.3*

Qualifier	Value
udp-src	UDP source port (0-65535)
udp-dst	UDP destination port (0-65535)
icmpv4-type	ICMPv4 type
icmpv4-code	ICMPv4 code
eth-type	"arp"/"0806" or "ip"/"0800" or (hex-value < =65535)
ip-proto	"tcp" or "udp" or 0-255
ip-dscp	IP DSCP (6 bits in ToS field)
arp-op	"request" or "reply" (can be set only if eth-type is ARP)
mpls-label	MPLS label
all	all qualifiers or any qualifier

The following table describes the available actions:

Table 375. *Static Flow Actions in OpenFlow 1.0*

Action	Value
output	"all","in-port","controller" or a valid port
set-src-mac	Change source MAC address
set-dst-mac	Change destination MAC address
strip-vlan-id	Remove VLAN identifier
set-vlan-priority	Set 802.1p priority code point value (0-7)
set-nw-tos	Set IP Type of Service (0-255)
drop	Drop packet
max-len	Maximum length to send to controller

Table 376. *Static Flow Actions in OpenFlow 1.3*

Action	Value
output	"all","in-port","controller" or a valid port
output-portchannel	output on a valid portchannel (static LAG or static LACP LAG)
set-eth-src	change source MAC address
set-eth-dst	change destination MAC address
push-vlan	push a new VLAN tag
pop-vlan	pop the outer VLAN tag

Table 376. *Static Flow Actions in OpenFlow 1.3 (continued)*

Action	Value
push-mpls	push a new MPLS tag
pop-mpls	pop the MPLS tag
set-vlan-vid	set VLAN ID
set-vlan-pcp	set 802.1p priority (0-7)
set-ip-dscp	set IP Differentiated Services Code Point (0-63)
set-mpls-label	set MPLS label <1-0xFFFFF)
set-mpls-ttl	set MPLS time-to-live
copy-ttl-out	copy time-to-live outward - from next-to-outermost to outermost
copy-ttl-in	copy time-to-live inward - from outermost to next-to-outermost
dec-nw-ttl	decrement network time-to-live
drop	drop the packet

Precision Time Protocol Configuration

Precision Time Protocol (PTP) allows high accuracy clock synchronization between a networked master clock and compliant network hosts. The Lenovo RackSwitch G8272 supports two PTP modes:

- Ordinary slave clock - Synchronizes the Real Time Clock (RTC) with PTP master clocks detected on the network.
- End-to-End transparent clock - Allows PTP traffic to pass through without affecting the RTC, while updating the correction fields for event packets.

Table 377. *Precision Time Protocol Configuration Options*

Command Syntax and Usage
`[no] ptp ordinary enable` Enables or disables PTP ordinary slave clock mode. In this mode, if a PTP master clock is detected on the network, the RTC is synchronized with it. If no master clock is detected, the RTC is not affected. The default setting is `disabled`. **Note:** Enabling PTP ordinary slave clock mode disables NTP settings and system time clock manual settings. **Command mode:** Global configuration
`[no] ptp transparent enable` Enables or disables PTP End-to-End transparent clock mode. In this mode, incoming PTP packets are forwarded based on routing rules currently in place for the PTP domain's multicast address (within the 224.0.1.129 - 224.0.1.132 range). On egress, PTP packet timestamps are updated based on the time spent between ingress and egress. The default setting is `disabled`. **Command mode:** Global configuration
`ip ptp source-interface loopback` *<1-5>* Loopback interface used as source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode. By default, the interface with the lowest index from the master clock's VLAN is used. **Command mode:** Global configuration
`no ip ptp source-interface loopback` Sets source IP address for delay-request packets sent during synchronization with the master clock in ordinary slave mode to the interface with the lowest index from the master clock's VLAN. **Command mode**: Global configuration
`no ptp` Disables both PTP ordinary slave clock mode and PTP End-to-End transparent clock mode. **Command mode:** Global configuration

Table 377. *Precision Time Protocol Configuration Options (continued)*

Command Syntax and Usage
[no] ptp Enables or disables PTP on the current port. Disabled ports will not support PTP even if PTP is globally enabled. The default setting is `enabled`. **Note:** PTP is not supported on management ports. **Command mode**: Interface port
show ptp Displays current PTP settings. **Command mode**: All

Microburst Detection

Microbursts are short peaks in data traffic that manifest as a sudden increase in the number of data packets transmitted over a specific millisecond-level time frame, potentially overwhelming network buffers. Microburst detection allows users to analyze and mitigate microburst-related incidents, thus preventing network congestion.

Table 378. *Microburst Detection Configuration Options*

Command Syntax and Usage
`[no] microburst enable` Enables or disables microburst detection. The default setting is `disabled`. **Command mode:** Global configuration
`microburst interval` *<2-10000>* Configures microburst detection interval granularity in milliseconds. The default setting is `5` miliseconds. **Command mode:** Global configuration
`microburst port-threshold` *<port alias or number> <1-60628>* Configures the number of memory cells a port is allowed to access from the shared service pool. There is no dedicated number of memory cells for a port. If this threshold is reached, it means the port is congested and needs to access additional memory from the shared service pool. The default value is `60628`. **Command mode:** Global configuration
`show microburst microburst-status` Displays microburst state and, if applicable, bursting time for each port. **Command mode:** All
`show microburst pkt-stats` Displays memory cell usage for egress unicast and multicast packets, broken down by port and QoS queue. **Command mode:** All
`show microburst port-log` Displays memory cell allocation and usage for ingress packets on each port. **Command mode:** All

Service Location Protocol Configuration

Service Location Protocol (SLP) enables networked devices to request/announce services over a local area network without prior configuration. In an SLP environment, devices may have the following roles:

- User Agents (UA) are devices requesting services.
- Service Agents (SA) are devices providing services.
- Directory Agents (DA) are devices caching services provided by SAs. When present in an SLA setup, DAs mediate all communication between UAs and SAs.

When SLP is enabled, the RackSwitch G8272 behaves as a Service Agent providing systems management services.

Table 379. *Service Location Protocol Options*

Command Syntax and Usage
`[no] ip slp active-da-discovery enable` Enables or disables active directory agent discovery. The default value is `disabled`. **Command mode**: Global configuration
`ip slp active-da-discovery-start-wait-time` *<1-10>* Number of seconds to wait after enabling SLP before attempting active DA discovery, if active DA discovery is enabled. The default value is 3 seconds. **Command mode**: Global configuration
`[no] ip slp enable` Enables or disables SLP. The default value is `disabled`. **Command mode**: Global configuration
`clear ip slp directory-agents` Clears directory agents discovered. **Command mode**: Privileged EXEC
`show ip slp directory-agents` Displays DA information. **Command mode**: All
`show ip slp information` Displays SLP information. **Command mode**: All
`show ip slp user-agents` Displays UA information. **Command mode**: All

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
RS G8272# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via SFTP/FTP/TFTP, as described on page 677.

Saving the Active Switch Configuration

When the **copy running-config** command is used, the switch's active configuration commands (as displayed using **show running-config**) will be uploaded to the specified script configuration file on the FTP/TFTP/SFTP server. To start the switch configuration upload, at the prompt, enter:

```
RS G8272# copy running-config ftp
```

or:

```
RS G8272# copy running-config sftp
```

or:

```
RS G8272# copy running-config tftp
```

The switch prompts you for the server address and filename.

Note: The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

Note: If the FTP/TFTP/SFTP server is running SunOS or the Solaris operating system, the specified configuration file must exist prior to executing the `copy running-config` command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Restoring the Active Switch Configuration

When the **copy running-config** command is used, the active configuration will be replaced with the commands found in the specified configuration file. The file can contain a full switch configuration or a partial switch configuration.

To start the switch configuration download, at the prompt, enter:

```
RS G8272# copy ftp running-config
```

or:

```
RS G8272# copy sftp running-config
```

or:

```
RS G8272# copy tftp running-config
```

The switch prompts you for the server address and filename.

USB Copy

If a USB drive is inserted into the USB port, you can copy files from the switch to the USB drive, or from the USB drive to the switch. You also can boot the switch using software or configuration files found on the USB drive (see "USB Boot Configuration" on page 705).

Copy to USB

Use the following command to copy a file from the switch to the USB drive:

usbcopy tousb *<filename>* **{active|boot|crashdump|image1|image2| |onie-image|syslog}**

Command mode: Privileged EXEC

In this example, the active configuration file is copied to a directory on the USB drive:

```
RS G8272# usbcopy tousb a_folder/myconfig.cfg active
```

Copy from USB

Use the following command to copy a file from the USB drive to the switch:

usbcopy fromusb *<filename>* **{active|boot|image1|image2| |onie-image}**

Command mode: Privileged EXEC

In this example, the active configuration file is copied from a directory on the USB drive:

```
RS G8272# usbcopy fromusb a_folder/myconfig.cfg active
```

The new file replaces the current file.

Note: Do not use two consecutive dot characters (..). Do not use a slash character (/) to begin a filename.

Python Scripting Configuration

Python Scripting allows the user to create his own running programs on the switch. These scripts allow the switch to perform the following:

- monitoring tasks
- automatically provision itself
- automatically upgrade switch firmware/generate configuration files

The following sections describe the Python Scripting configuration options.

- "Python Scripts Management and Execution" on page 680
- "Scheduler Jobs Management" on page 682
- "Running Job Monitor" on page 685

Python Scripts Management and Execution

The user can perform various script management actions: edit or delete a script, display script content.

In addition, the switch administrator may access Python shell and directly run a script.

The following table describes the Python Scripts Management and Execution commands.

Table 380. *Python Scripts Management and Execution Commands*

Command Syntax and Usage
copy script tftp [address *<IPv4 address>***] [filename** *<script filename>***] [data-port|mgt-port]** Creates a copy of the script on a TFTP server. **Command mode**: Privileged EXEC
copy script-log tftp [address *<IPv4 address>***] [filename** *<script log filename>***] [data-port|mgt-port]** Creates a copy of the script-log on a TFTP server. **Command mode**: Privileged EXEC
copy tftp script [address *<IPv4 address>***] [filename** *<script filename>***] [data-port|mgt-port]** Copies a script from a TFTP server. **Command mode**: Privileged EXEC
edit script *<script filename>* Creates or modifies a script via VI text editor. **Command mode**: All

Table 380. *Python Scripts Management and Execution Commands*

Command Syntax and Usage
no script <*script filename*> Deletes a script from the system. **Note**: If the script is specified as action of a scheduled job, the corresponding scheduled job must be deleted first. **Command mode**: Privileged EXEC
no script-log [<*script log filename*>**]** Deletes all script execution log files or a specific script log file from the system. **Command mode**: Privileged EXEC
python Provides access to Python shell. **Command mode**: Privileged EXEC
python <*script filename*> **[**<*argument list*>**]** Executes a python script directly. The optional list of arguments, if present, must be provided as a string enclosed in double quotes and the arguments must be separated by white spaces. The string representing the list of arguments must not exceed `199` characters. **Command mode**: Privileged EXEC
[no] logging log scheduler Enables or disables scheduler module syslog. The default setting is `enabled`. **Command mode**: Global Configuration
[no] logging log script Enables or disables scripting module syslog. The default setting is `enabled`. **Command mode**: Global Configuration
show script [<*script filename*>**]** Displays a list of all installed scripts or a specific script. **Command mode**: All
show script-log [<*script log filename*>**]** Displays a list of all script log files or a specific script log file. **Note**: All script-log files are automatically deleted after a reboot of the switch. **Command mode**: All

Scheduler Jobs Management

The user is allowed to define up to 20 scheduler jobs as a mapping of event and action. When the specified event occurs, the corresponding script is executed.

Table 381. *Scheduler Jobs Management Configuration Commands*

Command Syntax and Usage
scheduler job name *<job name>* Creates a scheduler job and Scheduler Job command mode. **Note**: A scheduler job can be created prior to downloading/creating an actual script. **Command mode**: Global configuration
action *<script file name>* **[***<argument list>***]** Configures the script file name to be executed and an optional list of arguments that are passed to the script when executed. The list of arguments must be provided as a string enclosed in double quotes and the arguments must be separated by white spaces. The arguments string must not exceed 199 characters. **Command mode**: Scheduler Job
event counter cpu ge *<1-99>* Triggers a script execution when CPU usage percentage exceeds an user defined threshold. CPU usage percentage is checked every 60 seconds. **Command mode**: Scheduler Job
event counter interface port *<1-48>* **{in-discard|out-discard} ge** *<1-2147483647>* **[interval** *<10-300>***]** Triggers a script execution when the number of discarded frames per second on a port is greater than or equal to the set up value. When an interval value is configured, the discarded frames rate is averaged over a configured period of time instead of a fixed interval 60 seconds. **Command mode**: Scheduler Job
event counter interface port *<1-48>* **{in-error|out-error} ge** *<1-2147483647>* **[interval** *<10-300>***]** Triggers a script execution when the number of errors on a port is greater than or equal to the set up value. When an interval value is configured, the error frames rate is averaged over a configured period of time instead of a fixed interval 60 seconds. **Command mode**: Scheduler Job
event counter memory ge *<1-50>* Triggers a script execution when memory usage percentage exceeds an user defined threshold. Memory usage percentage is checked every 60 seconds. **Command mode**: Scheduler Job

Table 381. *Scheduler Jobs Management Configuration Commands*

Command Syntax and Usage
event syslog *<event type>* Configures the syslog event which triggers the scheduled job. The following syslog event types are allowed: o **BGPSESDOWN** (BGP neighbor session failed event) o **BGPSESUP** (BGP neighbor session established event) o **DOT1XFAIL** (802.1x authentication failure event) o **ISLVLGDOWN** (vLAG ISL down event) o **ISLVLGUP** (vLAG ISL up event) o **LINKDOWN** (port link down event) o **LINKUP** (port link up event) o **LLDPDISCOVER** (LLDP neighbor add or delete event) **Note**: When a LLDP trap is detected, the scheduler automatically triggers a job. o **LOGINFAIL** (switch user login fail event) o **LOGINSUCC** (switch user login success event) o **MBURST** (microburst) **Note**: All ports microburst state is checked every 10 seconds. When a port goes into bursting state, the scheduler automatically triggers a job. o **MGTGWDOWN** (Mgmt gateway unavailable event) o **MGTGWUP** (Mgmt gateway available event) o **MROUTERNEW** (new multicast router learned event) o **STGTPCH** (STG topology change event) o **VRRPBKP** (VRRP becoming backup event) o **VRRPMRS** (VRRP becoming master event) **Note:** In order to trigger an event, the syslog for each corresponding event type must be enabled. **Command mode**: Scheduler Job
event time absolute *<yyyy> <mm> <dd> <hh:mm:ss>* **[interval [***<5-86400>***|***<hh:mm:ss>***]]** Triggers a script execution at a specific given date. The script runs only once if no time interval is configured. **Note**: If system time zone changes, all absolute timer jobs are automatically rescheduled. **Command mode**: Scheduler Job

Table 381. *Scheduler Jobs Management Configuration Commands*

Command Syntax and Usage
event time relative *<0-2147483647>* **[interval [***<5-86400>***| |***<hh:mm:ss>***]]** Triggers a script execution at a future start time expressed in seconds. The script runs only once if no time interval is configured. **Note**: When this command is applied, the relative time is automatically converted to absolute time. Thus, the event is visible in running configuration as an absolute time. **Command mode**: Scheduler Job
no scheduler job name *<job name>* Deletes the specified scheduler job. **Command mode:** Global configuration
show scheduler job [name *<job name>***]** Displays a list of all currently scheduled jobs or detailed information about a specified scheduled job. For more information, see page page 209. **Command mode**: All

Running Job Monitor

The user is allowed to control running scripts.

The following table describes the job monitoring commands.

Table 382. *Running Job Monitor Configuration Commands*

Command Syntax and Usage
kill scheduler job name *<job name>* Terminates a running script. **Command mode**: Privileged EXEC
scheduler job cpu-limit *<5-50>* Enables the option to terminate a running script when CPU usage percentage exceeds a globally defined threshold. By default, CPU usage percentage is checked every 5 seconds. **Command mode**: Global configuration
no scheduler job cpu-limit Disables the option to terminate a running script when CPU usage percentage exceeds a globally defined threshold. **Command mode:** Global configuration
scheduler job time-limit *<10-600>* Enables the option to terminate a running script when elapsed time exceeds a globally defined threshold (seconds). **Command mode**: Global configuration
no scheduler job time-limit Disables the option to terminate a running script when elapsed time exceeds a globally defined threshold. **Command mode:** Global configuration
show scheduler job cpu-limit Displays configured CPU usage limit value. **Command mode**: All
show scheduler job running Displays information about all currently running scripts. **Command mode:** All
show scheduler job time-limit Displays configured elapsed time limit value. **Command mode**: All

Chapter 5. Operations Commands

Operations commands generally affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use Operations commands to immediately disable a port (without the need to apply or save the change), with the understanding that when the switch is rebooted, the port returns to its normally configured operation.

These commands enable you to alter switch operational characteristics without affecting switch configuration.

Table 383. *General Operations Commands*

Command Syntax and Usage
`access tnetsshc` Closes all open Telnet and SSH connections. **Command Mode**: Global configuration
`console-log` Enables or disables session console logging. **Command Mode**: Privileged EXEC
`ntp send` Allows the user to send requests to the NTP server. **Command Mode**: Privileged EXEC
`password` *<1-128 characters>* Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters. **Command Mode**: Privileged EXEC
`clear logging` Clears all Syslog messages. **Command Mode**: Privileged EXEC
`clear openflow table [basic|emergency|static]` Clears OpenFlow tables. o The `basic` option clears only the basic OpenFlow table. o The `emergency` option clears only the emergency OpenFlow table. o The `static` option clears only the static Openflow table. **Command Mode**: Privileged EXEC

Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 384. *Port Operations*

Command Syntax and Usage
interface port *<port alias or number>* **dot1x init** Reinitializes 802.1x access control on the port. **Command Mode**: Privileged EXEC
interface port *<port alias or number>* **dot1x re-authenticate** Immediately starts reauthentication on the port. **Command Mode**: Privileged EXEC
[no] interface port *<port alias or number>* **rmon** Temporarily enables or disables remote monitoring of the port. The port will be returned to its configured operation mode when the switch is rebooted. **Command Mode**: Privileged EXEC
interface port *<port alias or number>* **shutdown** Temporarily disables the port. The port will be returned to its configured operation mode when the switch is rebooted. **Command Mode**: Privileged EXEC
no interface port *<port alias or number>* **shutdown** Temporarily enables the port. The port will be returned to its configured operation mode when the switch is rebooted. **Command Mode**: Privileged EXEC
show interface port *<port alias or number>* **operation** Displays the port interface operational state. **Command Mode**: All

Operations-Level NAT Commands

NAT operations commands are listed in the following table.

Table 385. *NAT Operations*

Command Syntax and Usage
clear ip nat statistics Clears NAT statistics. **Command Mode**: Privileged EXEC
clear ip nat translations Clears dynamically created NAT translations. **Command Mode**: Privileged EXEC

Operations-Level VRRP Commands

VRRP operation commands are listed in the following table.

Table 386. *Virtual Router Redundancy Operations*

Command Syntax and Usage
`router vrrp backup group` Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases: o This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same). o This switch's virtual router has a higher priority and preemption is enabled. o There are no other virtual routers available to take master control. **Command Mode**: Privileged EXEC

VMware Operations

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (**`virt vmware vcspec`**).

Table 387. *VMware Operations*

Command Syntax and Usage
`virt vmware export` *<VM profile name> <VMware host ID> <Virtual Switch name>* Exports a VM Profile to a VMware host. Use one of the following identifiers to specify each host: o UUID o IP address o Host name You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch. **Command Mode**: All
`virt vmware pg` *<Port Group name> <host ID> <VSwitch name> <VLAN ID (0-4094)> <shaping-enabled>* **[***<average-Kbps> <burst-KB> <peak-Kbps>***]** Adds a Port Group to a VMware host. You are prompted for the following information: o Port Group name o VMware host ID (Use host UUID, host IP address, or host name.) o Virtual Switch name o VLAN ID of the Port Group o Whether to enable the traffic-shaping profile (`1` or `0`). If you choose `1` (yes), you are prompted to enter the traffic shaping parameters. **Command Mode**: All
`no virt vmware pg` *<Port Group name> <host ID>* Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All
`virt vmware scan` Performs a scan of the VM Agent, and updates VM information. **Command Mode**: All

Table 387. *VMware Operations (continued)*

Command Syntax and Usage
virt vmware updpg *<Port Group name> <host ID> <VLAN ID (0-4094)>* **[***<shaping enabled> <average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>***]** Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID: o UUID o IP address o Host name Enter the traffic shaping parameters as follows: o Shaping enabled o Average traffic, in kilobits per second o Maximum burst size, in kilobytes o Peak traffic, in kilobits per second Delete traffic shaping parameters. **Command Mode**: All
virt vmware vmacpg *<VM NIC MAC address> <Port Group name>* Changes a VM NIC's configured Port Group. **Command Mode**: All
[no] virt vmware vsw *<host ID> <Virtual Switch name>* Adds or removes a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All

VMware Distributed Virtual Switch Operations

Use these commands to administer a VMware Distributed Virtual Switch (dvSwitch).

Table 388. *VMware dvSwitch Operations (/oper/virt/vmware/dvswitch)*

Command Syntax and Usage
virt vmware dvswitch add *<datacenter name> <dvSwitch name>* **[***<dvSwitch version>***]** Adds the specified dvSwitch to the specified DataCenter. **Command Mode**: All
virt vmware dvswitch addhost *<dvSwitch name>* **{***<host UUID***|** **|***host IP address***|***host name>**}*** Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All
virt vmware dvswitch adduplink *<dvSwitch name>* **{***<host UUID***|** **|***host IP address***|***host name>**}** *<uplink name>* Adds the specified physical NIC to the specified dvSwitch uplink ports. **Command Mode**: All
virt vmware dvswitch del *<datacenter name> <dvSwitch name>* Removes the specified dvSwitch from the specified DataCenter. **Command Mode**: All
virt vmware dvswitch remhost *<dvSwitch name>* **{***<host UUID***|** **|***host IP address***|***host name>**}*** Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode:** All
virt vmware dvswitch remuplink *<dvSwitch name>* **{***<host UUID***|** **|***host IP address***|***host name>**}*** *<uplink name>* Removes the specified physical NIC from the specified dvSwitch uplink ports. **Command Mode**: All

VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

Table 389. *VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)*

Command Syntax and Usage
virt vmware dpg add *<port group name> <dvSwitch name> <VLAN ID (1-4094)>* **[ishaping** *<bandwidth> <burst size> <peak bandwidth>***] [eshaping** *<bandwidth> <burst size> <peak bandwidth>***]** Adds the specified port group to the specified dvSwitch. You may enter the following parameters: o **ishaping**: Enables ingress shaping. Supply the following information: • average bandwidth in kilobits per second • burst size in kilobits • peak bandwidth in kilobits per second o **eshaping**: Enables engress shaping. Supply the following information: • average bandwidth in kilobits per second • burst size in kilobits • peak bandwidth in kilobits per second **Command Mode**: All
virt vmware dpg del *<port group name> <dvSwitch name>* Removes the specified port group from the specified dvSwitch. **Command Mode**: All
virt vmware dpg update *<port group name> <dvSwitch name> <VLAN ID (1-4094)>* **[ishaping** *<bandwidth> <burst size> <peak bandwidth>***] [eshaping** *<bandwidth> <burst size> <peak bandwidth>***]** Updates the specified port group on the specified dvSwitch. You may enter the following parameters: o **ishaping**: Enables ingress shaping. Supply the following information: • average bandwidth in kilobits per second • burst size in kilobytes • peak bandwidth in kilobits per second o **eshaping**: Enables egress shaping. Supply the following information: • average bandwidth in kilobits per second • burst size in kilobytes • peak bandwidth in kilobits per second **Command Mode**: All
virt vmware dpg vmac *<VNIC MAC> <port group name>* Adds the specified VM NIC to the specified port group. **Command Mode**: All

Edge Virtual Bridge Operations

Edge Virtual Bridge operations commands are listed in the following table:

Table 390. *Edge Virtual Bridge Operations Commands*

Command Syntax and Usage
virt evb update vsidb *<VSIDB number>* Update VSI types from the VSI database. **Command mode**: All
clear virt evb vsi [mac-address|port *<port alias or number>***|** **|type-id** *<1-16777215>***|vlan** *<1-4094>***]** Clears VSI database associations. **Command mode**: Privileged EXEC
clear virt evb vsidb [mgrid *<0-255>***|type-id** *<1-16777215>***|** **|version** *<0-255>***]** Clears local VSI types cache. **Command mode**: Privileged EXEC

Chapter 6. Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch on the next reboot
- Selecting a configuration block to be used when the switch on the next reboot
- Downloading or uploading a new software image to the switch via SFTP/FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files”.

The boot options are discussed in the following sections.

Scheduled Reboot of the Switch

This feature allows the switch administrator to schedule a reboot to occur at a particular time in future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the current reboot schedule.

Table 391. *Scheduled Reboot Options*

Command Syntax and Usage
boot schedule *<day> <time (hh:mm)>* Configures the switch reboot time. The following options are valid for the day value: o monday o tuesday o wednesday o thursday o friday o saturday o sunday **Command mode**: Global configuration
no boot schedule Cancels the switch reboot time. **Command mode**: Global configuration
show boot Displays the current switch reboot schedule. **Command mode**: All

Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

Table 392. *Netboot Options*

Command Syntax and Usage
boot netboot cfgfile *<1-31 characters>* Defines the file path for the configuration file or script file on the TFTP server. For example: o `/directory/sub/config.cfg` o `/directory/sub/config.py` **Command mode**: Global configuration
no boot netboot cfgfile Removes the file path for the configuration file or script file on the TFTP server. **Command mode:** Global configuration
[no] boot netboot enable Enables or disables Netboot. When enabled, the switch boots into factory-default configuration and attempts to download a new configuration file. **Command mode**: Global configuration
[no] boot netboot tftp *<IP address>* Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled or if the DHCP server does not return the required information. **Command mode**: Global configuration
show boot Displays the current Netboot parameters. **Command mode**: All

Security Policy Configuration

The switch can be configured to use two different security modes:

- Legacy policy mode
- Secure policy mode

Legacy Policy mode allows the switch to use all communication protocols with no regards to the security level of the protocol.The switch will be able to use both protocols that encrypt and do not encrypt their communication across the network.

Secure Policy mode allows the switch to use only secure communication protocols. Protocols that are regarded as being insecure are disabled and cannot be run on the switch. The commands associated with such protocols are unavailable.

The following protocols are disabled and are not available on the switch if Secure Policy mode is enabled:

- HTTP
- LDAP Client
- SNMPv1 and SNMPv2
- Telnet Client and Telnet Server
- Telnet IPv6 Client and Telnet IPv6 Server
- FTP Client and FTP Server
- Radius Client
- TACACS+ Client
- Syslog Server

The following protocols are enabled and available on the switch if Secure Policy mode is enabled:

- DHCP Client
- DHCPv6 Client
- Syslog

The following protocols are disabled, but are available on the switch even if Secure Policy mode is enabled:

- TFTP Server and TFTP Client (only for signed software images)

The following protocols are regarded as secure. They are enabled on the switch in both security modes and can be disabled:

- SCP Server
- SNMPv3 Client
- SFTP Client
- SSHv2 Client and SSHv2 Server
- HTTPS Server

The following protocols are regarded as secure. They are enabled on the switch in both security modes, but cannot be disabled:

- NTP Client version 4
- LDAPS Client

The following protocols are unaffected by Secure Policy Mode:

- SLP Discovery
- IKE
- IPSec
- Ping and Ping IPv6
- Traceroute and Traceroute IPv6
- bootp
- TFTP IPv6
- SNMPv3 IPv6

To configure the switch policy mode, use the following command:

Table 393. *Security Policy Configuration*

Command Syntax and Usage
boot security-policy {legacy-mode|secure-mode} Configures the switch security policy. **Note**: A switch reload is needed for the changes to take effect. **Command mode**: Global configuration
show boot security-policy Displays the current security policy configuration. **Command mode**: All

Configuring the Number of Spanning Tree Groups

The maximum number of Spanning Tree Groups (STGs) available on the switch can be configured to be either 128 or 256.

Table 394. *Configuring the Maximum Number of STGs Command Options*

Command Syntax and Usage
boot spanning-tree max-instances {128|256} Configures the maximum number of Spanning Tree Groups (STGs) that can be used on the switch. The default value is 128. **Note**: The switch needs to be reloaded for the configuration to take effect. **Command mode**: Global configuration
no boot spanning-tree max-instances Reset the maximum number of STGs available on the switch to the default value of 128. **Note**: The switch needs to be reloaded for the configuration to take effect. **Command mode**: Global configuration
show boot spanning-tree Displays the maximum number of currently available STGs on the switch and the maximum number of available STGs after the switch reloads. **Command mode**: All

The following command displays the current maximum limit of STGs on the switch and the maximum limit configured after the switch reloads:

show boot spanning-tree

Command mode: All

```
Bootup Max PVRST Instances: 128
Saved  Max PVRST Instances: 256

NOTE: A Reboot is required for the new settings to take effect.
      When switching from 256 to 128 STP instances, please remove any
      extra configuration for STP instance 128 and above, then save
      the configuration;  otherwise, all STP instance configuration
      may be lost after reload.
```

Machine Type Model Configuration

This feature configures the switch Machine Type Model (MTM).

Table 395. *Machine Type Model Configuration*

Command Syntax and Usage
boot mtm *<MTM code>* Configures the switch's machine type model (MTM) value. MTMs are applied on reboot and persist over firmware upgrades: **Command mode**: Global configuration

QSFP Port Configuration

The following table displays the QSFP Port configuration commands.

Table 396. *QSFP Port Options*

Command Syntax and Usage
[no] boot qsfp-40gports *<port alias or number>* Enables or disables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports. **Note:** You must reboot the switch for this change to take effect. **Command mode**: Global configuration
show boot qsfp-port-modes Displays the current QSFP parameters. **Command mode**: All

USB Boot Configuration

USB Boot allows you to boot the switch with a software image file, boot file or configuration file that resides on a USB drive inserted into the USB port. Use the following command to enable or disable USB Boot:

`[no] boot usbboot enable`

Command mode: Global configuration

Note: Not available in stacking.

When enabled, the switch checks the USB port when it is rebooted. If a USB drive is inserted into the port, the switch checks the drive for software and image files. If a valid file is present on the USB drive, the switch loads the file and boots using the file.

The following list describes the valid file names and describes the switch behavior when it recognizes them. The file names must be exactly as shown or the switch will not recognize them.

- `RSG8272_Boot.img`
  The switch replaces the current boot image with the new image and boots with the new image.
- `RSG8272_OS.img`
  The switch boots with the new software image. The existing images are not affected.
- `RSG8272_replace1_OS.img`
  The switch replaces the current software image1 with the new image and boots with the new image.
- `RSG8272_replace2_OS.img`
  The switch replaces the current software image2 with the new image and boots with the new image.
- `RSG8272.cfg`
  The switch boots with the new configuration file. The existing configuration files (active and backup) are not affected.
- `RSG8272_replace.cfg`
  The switch replaces the active configuration file with the new file and boots with the new file. This file takes precedence over any other configuration files that may be present on the USB drive.

If more than one valid file is present, the switch loads all valid files and boots with them. For example, you may simultaneously load a new boot file, image file and configuration file from the USB drive.

The switch ignores any files that do not match the valid file names or that have the wrong format.

You also can copy files to and from the USB drive. See "USB Copy" on page 679.

To safely remove the USB device without corrupting any files, use the following command:

`system usb-eject`

Command mode: Global configuration

Note: Not available in stacking.

Updating the Switch Software Image

The switch software image is the executable code running on the RackSwitch G8272. A version of the image ships with the switch and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch.

Use the following command to determine the current software version:

```
show boot
```

Command mode: All

Upgrading the software image on your switch requires the following:

- Loading the new image onto a SFTP, FTP, or TFTP server on your network
- Transferring the new image from the SFTP, FTP, or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is rebooted

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2` or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on a SFTP/FTP/TFTP server on your network
- The hostname or IP address of the SFTP/FTP/TFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

```
RS G8272# copy {ftp|tftp|sftp} {image1|image2|boot-image}
```

2. Select a port to use for downloading the image.

```
Port type [DATA|MGT]:
```

3. Enter the hostname or IP address of the SFTP, FTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

4. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

   The exact form of the name will vary by server. However, the file location is normally relative to the SFTP, FTP or TFTP directory (usually `tftpboot`).

5. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

6. The system prompts you to confirm your request.

   Next, select a software image to run, as described in the following section.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
RS G8272(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot.

   The system informs you of which image set to be loaded at the next reboot:

```
Next boot will use switch software image1 instead of image2.
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a SFTP, FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
RS G8272# copy {image1|image2|boot-image} {ftp|tftp|sftp}
```

2. Select a port type to use for uploading the image.

```
Port type [DATA|MGT]:
```

3. Enter the name or the IP address of the SFTP, FTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

4. Enter the name of the file into which the image will be uploaded on the SFTP, FTP or TFTP server:

```
Destination file name: <filename>
```

5. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

6. The system then requests confirmation of what you have entered. To have the file uploaded, enter **Y**.

```
image2 currently contains Software Version 6.6.0
 that was downloaded at  0:23:39 Thu Jan  3, 2011.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the RackSwitch G8272, you must save the changes so that they are retained beyond the next time the switch is rebooted. When you perform a save operation, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your RackSwitch G8272 was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured RackSwitch G8272 is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is rebooted:

```
RS G8272(config)# boot configuration-block {active|backup|factory}
```

Setting an Entitlement Serial Number

To improve customer technical support, your customer support representative can assign your switch an Entitlement Serial Number (ESN) at the time you request support. The ESN can be conveniently stored on the switch using the following command:

```
RS G8272(config)# boot esn <Entitlement Serial Number>
```

The ESN helps to locate your switch's identifying information when you call technical support for help in future.

Rebooting the Switch

You can reboot the switch to make your software image file and configuration block changes occur.

Note: Rebooting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

Enter the following command to reboot (reload) the switch:

```
RS G8272# reload [no-dump]
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.
>> Note that this will RESTART the Spanning Tree,
>> which will likely cause an interruption in network service.
Confirm reload (y/n) ?
```

Note: Before rebooting, the switch writes (saves) technical support information (backup-tech-support) in a local file to flash memory. The `no-dump` option skips this step, thereby decreasing the time needed for the switch to reboot. By default, the switch saves technical support information before rebooting.

Technical support information (backup-tech-support) can be uploaded to an external server using the following command:

`copy backup-tech-support {ftp|sftp|tftp}`

Command mode: Privileged EXEC

Note: Technical support information is stored in a compressed format. For details, see page 723.

Changing the Switch Profile

The Enterprise NOS software for the G8272 can be configured to operate in different modes for different deployment scenarios. The deployment profile changes some of the basic switch behavior, shifting switch resources to optimize capacity levels to meet the needs of different types of networks. For more information about deployment profiles, see the *Lenovo RackSwitch G8272 Application Guide for Lenovo Enterprise Network Operating System 8.4*.

To change the deployment profile, select the new profile and reboot the G8272. Use the following command to select a new profile:

```
RS G8272(config)# boot profile {acl|default|ipmc-opt|openflow}
```

The following list describes the boot profile options:

- `acl` - deployment profile with maximum Access Control Lists (ACLs)
- `default` - deployment profile with balanced resources
- `ipmc-opt` - deployment profile with different IPMC entries and ACLs:
  - `acls-none` - 1792 IPMC entries and no ACLs
  - `acls-128` - 1536 IPMC entries and 128 ACLs
  - `acls-256` - 1280 IPMC entries and 256 ACLs
  - `acls-384` - 1024 IPMC entries and 384 ACLs
- `openflow` - OpenFlow Only deployment profile

ONIE

The Open Network Install Environment (ONIE) is a small Linux-based operating system that provides an open install environment for network switches without operating systems.

ONIE enables a network switch ecosystem where end-users can choose among different Network Operating Systems (NOS). Practically, ONIE boots on a switch, discovers NOS installer images available on the local network or USB drive, copies the chosen image to the switch, and provides an environment where the installer can load the NOS onto the switch.

Note: ONIE commands are available only after you have installed the ONIE license key. For more details, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*.

Table 397. *ONIE Command Options*

Command Syntax and Usage
boot image onie-image install Configures the switch to reload in ONIE install mode, which is used to install a NOS image on the switch. **Command mode**: Global configuration
boot image onie-image rescue Configures the switch to reload in ONIE rescue and recovery mode, which is useful when trying to recover from a broken NOS image. **Command mode**: Global configuration
boot image onie-image uninstall Configures the switch to reload in ONIE uninstall mode, which is used to remove the Network Operating System image from the switch. **Command mode**: Global configuration
boot image onie-image update Configures the switch to reload in ONIE update mode, which is used to update the ONIE image. **Note**: This will also install a different version of the ONIE boot loader, which does not support running Lenovo Enterprise Network Operating System. If you wish to boot Enterprise NOS, you will have to re-install it by using ONIE Install mode. **Command mode**: Global configuration
show boot Displays the current switch reboot schedule. **Command mode**: All

Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift + B>**. The Boot Management menu appears.

```
Boot Management Menu
        M - Change boot mode (ENOS vs CNOS)
        I - Change booting image
        C - Change configuration block
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        O - ONIE submenu
        Q - Reboot
        E - Exit
Please choose your menu option:
```

The Boot Management menu allows you to perform the following actions:

- To change the startup mode, press **M** and follow the screen prompts. ENOS refers to Lenovo Enterprise Network OS (8.4 or prior) and CNOS refers to Lenovo Cloud Network OS (10.1 or later).
- To change the booting image, press **I** and follow the screen prompts.
- To change the configuration block, press **C** and follow the screen prompts.
- To boot in recovery mode press **R**. For more details see "Boot Recovery Mode" on page 716.
- To enter the ONIE submenu, press **O**.
- To restart the boot process from the beginning, press **Q**.
- To exit the Boot Management menu, press **E**. The booting process continues.

Note: The ONIE submenu will only be available if you have activated ONIE by installing an appropriate license key.

Boot Recovery Mode

The Boot Recovery Mode allows you to recover from a failed software or boot image upgrade using TFTP or XModem download.

To enter Boot Recovery Mode you must select "Boot in recovery mode" option from the Boot Management Menu by pressing **R**.

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option? :
```

The Boot Recovery Mode menu allows you to perform the following actions:

- To recover from a failed software or boot image upgrade using TFTP, press **T** and follow the screen prompts. For more details, see "Recover from a Failed Image Upgrade using TFTP" on page 717.
- To recover from a failed software or boot image upgrade using XModem download, press **X** and follow the screen prompts. For more details, see "Recovering from a Failed Image Upgrade using XModem Download" on page 719.
- To enable the loading of an unofficial image, press **P** and follow the screen prompts. For more details, see "Physical Presence" on page 721.
- To check if the switch is ready to run NOSx software, press **F**. It performs a check to see if the filesystem is optimally partitioned and updates it accordingly.
- To restart the boot process from the beginning, press **R**.
- To exit Boot Recovery Mode menu, press **E**. The boot process continues.

Recover from a Failed Image Upgrade using TFTP

Use the following procedure to recover from a failed image upgrade using TFTP:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, SecureCRT or PuTTY) and input the proper host name (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting **R**. The Recovery Mode menu will appear.
5. To start the recovery process using TFTP, select **T**. The following message will appear:

```
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
```

6. Enter the IP address of the management port:

```
IP addr :
```

7. Enter the network mask of the management port:

```
Netmask :
```

8. Enter the gateway of the management port:

```
Gateway :
```

9. Enter the IP address of the TFTP server:

```
Server addr:
```

10. Enter the filename of the image:

```
Image Filename:
```

11. If the file is a software image, enter an image number:

```
Install image as image 1 or 2 (hit return to just boot image):
```

After the procedure is complete, the Recovery Mode menu will be re-displayed.

Below is an example of a successful recovery procedure using TFTP:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option? : t
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
IP addr :10.241.6.4
Netmask :255.255.255.128
Gateway :10.241.6.66
Server addr:10.72.97.135
Image Filename: G8272-8.4.1.0_OS.img
        Netmask : 255.255.255.128
        Gateway : 10.241.6.66
Configuring management port.....................
Installing image G8272-8.4.1.0_OS.img from TFTP server 10.72.97.135

Extracting images ... Do *NOT* power cycle the switch.
Installing Application: Image signature verified.
Install image as image 1 or 2 (hit return to just boot image): 2
Installing image as image2: 100%

Image2 updated succeeded
Updating install log. File G8272-8.4.1.0_OS.img installed from
10.72.97.135 at 15:29:30 on 12-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option? :
```

Recovering from a Failed Image Upgrade using XModem Download

Use the following procedure to recover from a failed image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, SecureCRT, or PuTTY) and select the following serial port characteristics:
   - Speed: 9600 bps
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting **R**. The Recovery Mode menu will appear.
5. Select **X** for Xmodem download. You will see the following display:

```
Running xmodem rescue.....
```

6. When you see the following message, change the Serial Port speed to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

7. Press **<Enter>** to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start Xmodem on your terminal emulator. You will see a display similar to the following:

```
... Waiting for the <Enter> key to be hit before the download can start...
CC
```

8. Select the image to download. Xmodem initiates the file transfer. When download is complete, you are asked to change the Serial Port speed back to 9600 bps:

```
Change the baud rate back to 9600 bps, hit the <ENTER> key
```

9. Press **<Enter>** to start installing the image. If the file is a software image, enter the image number:

```
Install image as image 1 or 2 (hit return to just boot image):
```

The image install will begin. After the procedure is complete, the Recovery Mode menu will be re-displayed.

```
Extracting images ... Do *NOT* power cycle the switch.
Installing Root Filesystem:
Image signature verified.  100%
Installing Kernel:
Image signature verified.  100%
Installing Device Tree:
Image signature verified.  100%
Installing Boot Loader:  100%
Updating install log. File image installed from xmodem at 18:06:02 on
13-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        F) Filesystem check
        R) Reboot
        E) Exit

Option? :
```

Boot image recovery is complete.

Physical Presence

Use the following procedure to enable the installation of unofficial images on the switch:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, SecureCRT or PuTTY) and input the proper host name (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting **R**. The Recovery Mode menu will appear.
5. To begin the Physical Presence procedure, select **P**. The following warning message will appear:

```
WARNING: the following test is used to determine physical presence and if
completed will put the switch in low security mode.
```

6. You will be prompted for confirmation:

```
Do you wish to continue y/n?
```

7. A security test will be performed. The system location (blue) LED will blink a number of times between 1 and 12. Enter that number:

```
Hit a key to start the test. The blue location LED will blink a number of
times.

...........
How many times did the LED blink?
```

8. After entering the correct number, the Recovery Mode menu will re-appear. To install an unofficial image use one of the following procedures:
   - TFTP (for details, see page 717)
   - XModem Download (for details, see page 719)

   Note: You have three attempts to successfully complete the security test. After three incorrect attempts, the switch will reboot.

   Note: After the test is completed, the switch will be put in low security mode. This mode will allow you to install unofficial images on the switch. To revert to normal security mode, you must reboot the switch or press **P** again in the Recovery Mode menu.

ONIE Submenu

The Boot Management menu offers a way to access ONIE and configure the switch to boot in different ONIE modes.

You can interrupt the startup process of the switch and enter the Boot Management menu from the serial console port. When the system displays the following message, press **<Shift + B>**. The Boot Management menu will appear.

```
Boot Management Menu
        M - Change boot mode (Legacy vs NextGen)
        I - Change booting image
        C - Change configuration block
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        O - ONIE submenu
        Q - Reboot
        E - Exit
Please choose your menu option:
```

Note: The ONIE submenu is available only if you have installed the ONIE license key. For more details on installing ONIE, see the *Lenovo Network ONIE Quick Start Guide for Lenovo Network Operating System*.

To enter the ONIE submenu, press **O**.

```
ONIE Menu
     I - Startup ONIE OS installer
     N - Startup NOS mode (system default)
     R - Startup ONIE rescue mode
     U - Startup ONIE self update mode
     D - Startup ONIE OS uninstaller
     E - Exit ONIE menu

Option? :
```

The ONIE submenu allows you to perform the following actions:

- To boot the switch in ONIE Install mode, press **I**.
- To boot the switch in ONIE Rescue mode, press **R**.
- To boot the switch in ONIE Update mode, press **U**.
- To boot the switch in ONIE Uninstall mode, press **D**.
- To boot the switch using the installed NOS image, press **N**.
- To exit the ONIE submenu and return to the Boot Management Menu, press **E**.

Chapter 7. Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the RackSwitch G8272 after any one of the following occurs:

- The watchdog timer forces a switch reboot. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

To use the maintenance commands, you must be logged in to the switch as the administrator.

Table 398. *General Maintenance Commands*

Command Syntax and Usage
copy flash-dump {tftp|ftp|sftp} {data-port|mgt-port} Saves the system dump information via TFTP, SFTP or FTP. For details, see page 742. **Command mode:** Privileged EXEC
copy *<switch filename>* **tftp address** *<TFTP server IP address>* **filename** *<TFTP server filepath>* **{data-port|mgt-port}** Uploads a file via TFTP. **Command mode:** Privileged EXEC
copy log {stfp|tftp} {data-port|mgt-port} Uploads the system log file (SYSLOG) via SFTP or TFTP. **Command mode:** Privileged EXEC
copy tech-support {ftp|sftp} {data-port|mgt-port} Uploads the technical support dump (tsdmp) to an external FTP/SFTP server. **Command mode:** Privileged EXEC
copy tech-support tftp address *<hostname or server IP address>* **filename** *<TFTP server filepath>* **{data-port|mgt-port}** Uploads the technical support dump (tsdmp) to an external TFTP server. **Command mode:** Privileged EXEC
copy backup-tech-support {ftp|sftp} {data-port|mgt-port} Uploads the technical support information saved before a switch reboot (backup-tech-support) to an external FTP/SFTP server. **Note**: Technical support information is stored in a compressed format. **Command mode:** Privileged EXEC

Table 398. *General Maintenance Commands (continued)*

Command Syntax and Usage
copy backup-tech-support tftp address *<hostname or server IP address>* **filename** *<TFTP server filepath>* **{data-port|mgt-port}** Uploads the technical support information saved before a switch reboot (backup-tech-support) to an external TFTP server. **Note**: Technical support information is stored in a compressed format. **Command mode:** Privileged EXEC
clear flash-dump Clears dump information from flash memory. **Command mode:** Privileged EXEC
clear logging Clears the system log file (SYSLOG). **Command mode:** Privileged EXEC
show tech-support [fcoe|l2|l3|link|port] Dumps all G8272 information, statistics and configuration. You can log the output (`tsdmp`) into a file. To filter the information, use the following options: o `fcoe` displays only FCoE-related information o `l2` displays only Layer 2-related information o `l3` displays only Layer 3-related information o `link` displays only link status-related information o `port` displays only port-related information **Command mode:** All except User EXEC

Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 399. *FDB Manipulation Options*

Command Syntax and Usage
show mac-address-table address *<MAC address>* Displays a single database entry by its MAC address. Enter the MAC address using one of the following formats: o xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56) o xxxxxxxxxxxx (such as 080020123456) **Command mode:** All
show mac-address-table interface port *<port alias or number>* Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table multicast Displays all Multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table private-vlan *<VLAN ID (2-4094)>* Displays all FDB entries on a single private VLAN. **Command mode:** All
show mac-address-table static Displays static entries in the FBD. **Command mode:** All
show mac-address-table vlan *<VLAN ID (1-4094)>* Displays all FDB entries on a single VLAN. **Command mode:** All
no mac-address-table {multicast|static} {all|*<MAC address>* *<VLAN ID (1-4094)>***}** Removes static FDB entries. **Command mode:** Global configuration
clear mac-address-table Clears the entire Forwarding Database from switch memory. **Command mode:** Privileged EXEC

Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reboot occurs

If the switch reboots for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 400. *Miscellaneous Debug Options*

Command Syntax and Usage
debug debug-flags This command sets the flags that are used for debugging purposes. **Command mode:** Privileged EXEC
debug dumpbt Displays the backtrace log. **Command mode:** Privileged EXEC
[no] debug lacp packet {receive|transmit|both} port *<port alias or number>* Enables or disables debugging for Link Aggregation Control Protocol (LACP) packets on selected ports running LACP. The following parameters are available: o `receive` filters only LACP packets received o `transmit` filters only LACP packets sent o `both` filters LACP packets either sent or received o `port` filters LACP packets sent/received on specific ports By default, LACP debugging is `disabled`. **Command mode:** Privileged EXEC
debug mp-snap Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reboot occurred. **Command mode:** Privileged EXEC
debug mp-trace Displays the Management Processor trace buffer. Header information similar to the following is shown: `MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748` The buffer information is displayed after the header. **Command mode:** Privileged EXEC

Table 400. *Miscellaneous Debug Options*

Command Syntax and Usage
`[no] debug spanning-tree bpdu [receive|transmit]` Enables or disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received. The following parameters are available: o `receive` filters only BPDU frames received o `transmit` filters only BPDU frames sent By default, STP BPDU debugging is `disabled`. **Command mode**: Privileged EXEC
`[no] debug spanning-tree tc` Enables or disables the display of messages relating to STP topology changes. **Command mode**: Privileged EXEC
`[no] debug tacacs-client` Enables or disables TACACS+ client debug messages. **Command mode:** Privileged EXEC
`clear flash-config` Deletes all flash configuration blocks. **Command mode:** Privileged EXEC

SSH Debugging

The following table describes the SSH debugging commands.

Table 401. *SSH Debugging Options*

Command Syntax and Usage
[no] debug ssh client all Enables or disables all SSH Client debug messages. **Command mode:** Privileged EXEC
[no] debug ssh client state Enables or disables SSH Client state debug messages. **Command mode:** Privileged EXEC
[no] debug ssh server all Enables or disables all SSH Server debug messages. **Command mode:** Privileged EXEC
[no] debug ssh server disconnect Enables or disables SSH Server disconnect debug messages. **Command mode:** Privileged EXEC
[no] debug ssh server msg Enables or disables SSH Server type and protocol debug messages. **Command mode:** Privileged EXEC
[no] debug ssh server packet Enables or disables SSH Server type, protocol and packet debug messages. **Command mode:** Privileged EXEC
[no] debug ssh server state Enables or disables SSH Server state debug messages. **Command mode:** Privileged EXEC

IPsec Debugging

The following table describes the IPsec debugging commands.

Table 402. *IPsec Debugging Options*

Command Syntax and Usage
[no] debug sec all Enables or disables all IP security debug messages. **Command mode:** Privileged EXEC
[no] debug sec crypto Enables or disables all IP security cryptographic debug messages. **Command mode:** Privileged EXEC
[no] debug sec ike Enables or disables all IP security IKEv2 debug messages. **Command mode:** Privileged EXEC
[no] debug sec info Displays the current security debug flag. **Command mode:** Privileged EXEC
[no] debug sec ipsec Enables or disables all IPsec debug messages. **Command mode:** Privileged EXEC

vLAG Debugging

The following table describes vLAG debugging commands.

Table 403. *vLAG Debugging Options*

Command Syntax and Usage
[no] debug vlag cfg Enable or disables vLAG configuration debug messages. **Command mode:** Privileged EXEC
[no] debug vlag fdb-database Enable or disables vLAG Forwarding Database debug messages. **Command mode:** Privileged EXEC
[no] debug vlag htlhchk Enable or disables vLAG Health Check debug messages. **Command mode:** Privileged EXEC
[no] debug vlag isl Enable or disables vLAG ISL debug messages. **Command mode:** Privileged EXEC
[no] debug vlag msg Enable or disables vLAG debug messages. **Command mode:** Privileged EXEC
[no] debug vlag portmgr Enable or disables vLAG Port Manager debug messages. **Command mode:** Privileged EXEC
[no] debug vlag sm Enable or disables vLAG State Machine debug messages. **Command mode:** Privileged EXEC
[no] debug vlag trunk Enable or disables vLAG aggregation debug messages. **Command mode:** Privileged EXEC
[no] debug vlag vrrp Enable or disables vLAG VRRP debug messages. **Command mode:** Privileged EXEC

BGP Debugging

The following table describes BGP debugging commands.

Table 404. *BGP Debugging Options*

Command Syntax and Usage
[no] debug bgp Enables or disables all BGP debug messages for all existing peers. **Command mode:** Privileged EXEC
[no] debug bgp *<IP address>* Enables or disables all BGP debug messages for the specified BGP neighbor. **Command mode:** Privileged EXEC
[no] debug bgp *<IP address>* **{in|out}** Enables or disables all inbound or outbound BGP debug messages for the specified BGP neighbor. **Command mode:** Privileged EXEC
[no] debug bgp {in|out} Enables or disables all inbound or outbound BGP debug messages. **Command mode:** Privileged EXEC
[no] debug bgp persistent Enables or disables saving BGP debug settings to running configuration. **Command mode:** Privileged EXEC
show debug bgp Displays the current BGP debug setting. **Command mode:** All

BGP Maintenance

The following table describes the BGP information commands.

Table 405. *Border Gateway Protocol Maintenance Options*

Command Syntax and Usage
show ip bgp debugging [last] Displays all BGP debugging entries. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp debugging *<IP address>* **[last]** Displays all BGP debugging entries for the specified neighbor. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp debugging *<IP address>* **ignored [last]** Displays BGP information for routers that have been ignored by the specified neighbor. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp debugging *<IP address>* **{in|out} [last]** Displays inbound or outbound BGP debugging updates for the specified neighbor. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp debugging ignored [last] Shows all BGP information for routers that have been ignored. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp debugging {in|out} [last] Displays inbound or outbound BGP debugging updates. If the `last` option is specified, displays the results starting with the last entry first. **Command mode:** All
show ip bgp information Displays the BGP routing table. **Command mode:** All
show ip bgp information *<IP address> <mask>* Displays the BGP information related to the specified route. **Command mode:** All
clear ip bgp debug-log Clears the entire BGP debug log from switch memory. **Command mode:** Privileged EXEC

DCBX Maintenance

The following table describes the DCBX maintenance commands.

Table 406. *DCBX Maintenance Commands*

Command Syntax and Usage
show cee information dcbx port *<port alias or number>* Displays DCBX feature information for the selected port. **Command mode:** All
show cee information dcbx port *<port alias or number>* **app_proto** Displays DCBX application protocol state-machine information. **Command mode:** All
show cee information dcbx port *<port alias or number>* **control** Displays information about the Control state machine for the selected port. **Command mode:** All
show cee information dcbx port *<port alias or number>* **ets** Displays DCBX ETS state-machine information. **Command mode:** All
show cee information dcbx port *<port alias or number>* **feature** Displays information about the Feature state machine for the selected port. **Command mode:** All
show cee information dcbx port *<port alias or number>* **pfc** Displays DCBX PFC state-machine information. **Command mode:** All
show dcbx receive *<port alias or number>* Displays the Type-Length-Value (TLV) list received in the DCBX TLV for the selected port. **Command mode:** All
show dcbx transmit *<port alias or number>* Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV for the selected port. **Command mode:** All

LLDP Cache Manipulation

The following table describes the LLDP cache manipulation commands.

Table 407. *LLDP Cache Manipulation Options*

Command Syntax and Usage
show lldp [information] Displays all LLDP information. **Command mode:** All
show lldp port *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
show lldp port *<port alias or number>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specified port. **Command mode:** All
show lldp port *<port alias or number>* **vport** *<1-8>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specified virtual port on the selected port. **Command mode:** All
show lldp receive Displays information about the LLDP receive state machine. **Command mode:** All
show lldp transmit Displays information about the LLDP transmit state machine. **Command mode:** All
show lldp remote-device [*<1-256>***|detail|port** *<port alias or number>***]** Displays information received from LLDP -capable devices. For more information, see page 65. **Command mode:** All
clear lldp Clears the LLDP cache. **Command mode:** Privileged EXEC

ARP Cache Maintenance

The following table describes the ARP cache maintenance commands.

Table 408. *Address Resolution Protocol Maintenance Options*

Command Syntax and Usage
show [ip] arp Shows all ARP entries. **Command mode:** All
show [ip] arp find *<IP address>* Shows a single ARP entry by IP address. **Command mode:** All
show [ip] arp interface port *<port number or alias>* Shows ARP entries on selected ports. **Command mode:** All
show [ip] arp reply Shows the list of IP addresses which the switch will respond to for ARP requests. **Command mode:** All
show [ip] arp vlan *<VLAN ID (1-4094)>* Shows ARP entries on a single VLAN. **Command mode:** All
clear arp Clears the entire ARP list from switch memory. **Command mode:** Privileged EXEC

Note: To display all or a portion of ARP entries currently held in the switch, you can also refer to "ARP Information" on page 90.

IP Route Manipulation

The following table describes the IP route manipulation commands.

Table 409. *IP Route Manipulation Options*

Command Syntax and Usage
debug route-map pbr Enables policy-based routing debugging. **Command mode:** Privileged EXEC
show ip route Shows all routes. **Command mode:** All
show ip route address *<IP address>* Shows a single route by destination IP address. **Command mode:** All
show ip route gateway *<IP address>* Shows routes to a default gateway. **Command mode:** All
show ip route interface *<1-128>* Shows routes on a single interface. **Command mode:** All
show ip route tag {address|bgp|broadcast|fixed|martian| |multicast|ospf|rip|static} Shows routes of a single tag. For a description of IP routing tags, see Table 40 on page 88. **Command mode:** All
show ip route type {broadcast|direct|indirect|local| |martian|multicast} Shows routes of a single type. For a description of IP routing types, see Table 39 on page 88. **Command mode:** All
clear ip route Clears the route table from switch memory. **Command mode:** Privileged EXEC

Note: To display all routes, you can also refer to "IP Routing Information" on page 87.

IGMP Snooping Maintenance

The following table describes the IGMP Snooping maintenance commands.

Table 410. *IGMP Multicast Group Maintenance Options*

Command Syntax and Usage
show ip igmp groups Displays information for all multicast groups. **Command mode:** All
show ip igmp groups address *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
show ip igmp groups detail *<IP address>* Displays detailed information about a single IGMP multicast group. **Command mode:** All
show ip igmp groups interface port *<port alias or number>* Displays all IGMP multicast groups on selected ports. **Command mode:** All
show ip igmp groups portchannel *<1-144>* Displays all IGMP multicast groups on a single Link Aggregation Group (LAG). **Command mode:** All
show ip igmp groups vlan *<VLAN ID (1-4094)>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
clear ip igmp groups Clears the IGMP group table. **Command mode:** Privileged EXEC

IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 411. *IGMP Multicast Router Maintenance Commands*

Command Syntax and Usage
show ip igmp mrouter [dynamic|interface|portchannel|static] Displays information for all Mrouters, all dynamic/static Mrouter ports installed or Mrouter ports specific to a specified interface/portchannel. **Command mode:** All
show ip igmp mrouter information Displays IGMP snooping information for all Mrouters. **Command mode:** All
show ip igmp mrouter vlan *<VLAN ID (1-4094)>* Displays IGMP Mrouter information for a single VLAN. **Command mode:** All
show ip igmp querier vlan *<VLAN ID (1-4094)>* Displays IGMP querier information for a single VLAN. **Command mode:** All
show ip igmp relay Displays IGMP relay information. **Command mode:** All
show ip igmp snoop igmpv3 Displays IGMPv3 snooping information. **Command mode:** All
clear ip igmp mrouter Clears the dynamic IGMP Mrouter port table. **Command mode:** Privileged EXEC

Networking Virtualization Maintenance

The following table describes the maintenance commands for Networking Virtualization (NWV).

Table 412. *Networking Virtualization Maintenance Commands*

Command Syntax and Usage
debug bfd counters Displays VXLAN encapsulated Bidirectional Forwarding Detection (BFD) statistics. **Command mode:** Privileged EXEC
debug bfd show-sess-by-index *<0-5000>* Displays Bidirectional Forwarding Detection (BFD) sessions by index. **Note**: Using `0` as the index will display all BFD sessions. **Command mode:** Privileged EXEC
show nwv ovsdb connection Displays OVSDB connection information. **Command mode**: Privileged EXEC

The following command displays OVSDB connection information:

show nwv ovsdb connection

Command mode: Privileged EXEC

```
Idx  Type         Peer              State  Inact. ms Backoff ms Latest Method
---  -----------  ----------------- ------ --------- ---------- ------------------
1    SSL (Active) 10.241.43.60:6640 ACTIVE 30000      8000      transact (comment)
2    SSL (Active) 10.241.43.61:6640 ACTIVE 30000      8000      monitor
3    SSL (Active) 10.241.43.62:6640 ACTIVE 30000      8000      transact (comment)
```

IPv6 Neighbor Cache Manipulation

The following table describes the IPv6 Neighbor Cache manipulation commands.

Table 413. *IPv6 Neighbor Cache Manipulation Options*

Command Syntax and Usage
show ipv6 neighbors Shows all IPv6 Neighbor Cache entries. **Command mode:** All
show ipv6 neighbors find *<IPv6 address>* Shows a single IPv6 Neighbor Cache entry by IP address. **Command mode:** All
show ipv6 neighbors interface port *<port alias or number>* Shows IPv6 Neighbor Cache entries on a single port. **Command mode:** All
show ipv6 neighbors static Shows static IPv6 Neighbor Cache entries. **Command mode:** All
show ipv6 neighbors vlan *<VLAN ID (1-4094)>* Shows IPv6 Neighbor Cache entries on a single VLAN. **Command mode:** All
clear ipv6 neighbors Clears all IPv6 Neighbor Cache entries from switch memory. **Command mode:** Privileged EXEC

IPv6 Route Maintenance

The following table describes the IPv6 route maintenance commands.

Table 414. *IPv6 Route Maintenance Options*

Command Syntax and Usage
show ipv6 route Shows all IPv6 routes. **Command mode:** All
show ipv6 route address *<IPv6 address>* Show a single route by destination IP address. **Command mode:** All
show ipv6 route gateway *<IPv6 gateway address>* Show routes to a single gateway. **Command mode:** All
show ipv6 route interface *<1-128>* Show routes on a single IP interface. **Command mode:** All
show ipv6 route static Show static IPv6 routes. **Command mode:** All
show ipv6 route summary Shows a summary of IPv6 route information. **Command mode:** All
show ipv6 route type {connected|static|ospf} Show routes of a single type. **Command mode:** All
clear ipv6 route Clears all IPv6 routes. **Command mode:** Privileged EXEC

TFTP, SFTP, or FTP System Dump Copy

Use these commands to copy (save) the system dump to a TFTP, SFTP or FTP server.

Note: If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified file must exist *prior* to executing the **copy flash-dump tftp** command (or **copy flash-dump sftp**) and must be writable (set with proper permission and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
RS G8272# copy flash-dump tftp <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via SFTP, enter:

```
RS G8272# copy flash-dump sftp <server filename>
```

You are prompted for the SFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
RS G8272# copy flash-dump ftp <server filename>
```

You are prompted for the FTP server IPv4 address or hostname, your *username* and *password*, and the *filename* of the target dump file.

Clearing Dump Information

To clear dump information from flash memory, enter:

```
RS G8272# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2011. Use show flash-dump
      uuencode to
      extract the dump for analysis and clear flash-dump to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Appendix A. Enterprise NOS System Log Messages

The RackSwitch G8272 uses the following syntax when outputting system log (syslog) messages:

<Time stamp> <IP/Hostname> <Log Label> <Thread ID>:*<Message>*

The following parameters are used:

- *<Timestamp>*

  The time of the message event is displayed in the following format:

  <month (3 characters)> <day> <hour (1-24)>:*<minute>*:*<second>*

  For example: `Aug 19 14:20:30`

- *<IP/Hostname>*

  The hostname is displayed when configured.

  For example: `1.1.1.1`

- *<Log Label>*

  The following types of log messages are recorded: `LOG_CRIT`, `LOG_WARNING`, `LOG_ALERT`, `LOG_ERR`, `LOG_NOTICE` and `LOG_INFO`.

- *<Thread ID>*

  This is the software thread that reports the log message.

  For example:
  `stg`, `ip`, `console`, `telnet`, `vrrp`, `system`, `web server`, `ssh`, `bgp`

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as `mgmt`, one of the following may be shown: `console`, `telnet`, `web server` or `ssh`.

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
BGP	session with <*IP address*> failed (bad event:<*event*>)
BGP	session with <*IP address*> failed <*reason*> Reasons: • Connect Retry Expire • Holdtime Expire • Invalid • Keepalive Expire • Receive KEEPALIVE • Receive NOTIFICATION • Receive OPEN • Receive UPDATE • Start • Stop • Transport Conn Closed • Transport Conn Failed • Transport Conn Open • Transport Fatal Error
BGP	session with <*IP address*> failed <*reason type*> : <*reason*> Reason Types: • FSM Error • Hold Timer Expired • Message Header Error • OPEN Message Error • UPDATE Message Error Reasons: • AS Routing Loop • Attr Flags Error • Attr Length Error • Auth Failure • Bad BGP Identifier • Bad HoldTime • Bad Length • Bad Peer AS • Bad Type • Conn Not Synced • Invalid Network Field • Invalid NEXTHOP Attr • Invalid ORIGIN Attr • Malformed AS_PATH • Malformed Attr List • Missing Well Known Attr • None • Optional Attr Error • Unrecognized Well Known Attr • Unsupported Opt Param • Unsupported Version
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
IP	cannot contact gateway <IP address>
IP	Dynamic Routing table is full
IP	Route table full
MGMT	Maximum number of login failures (<*threshold*>) has been exceeded.

Thread	LOG_ALERT Message (continued)
oflow	Switch is configured to function in Openflow Mode
oflow	Switch is configured to function in Normal Mode
oflow	WARNING! In Hybrid Mode with Openflow enabled, legacy switching features are not supported on Openflow ports. Features involving TCAM resources are not supported on all ports.
oflow	WARNING! In Openflow Only Mode, legacy switching features are not supported on all ports.
oflow	Openflow Instance <x> disabled
oflow	Openflow Instance <x> deleted
oflow	Openflow Instance <x>: No Controller Available for Connection
oflow	Openflow Instance <x>: Failed to receive Hello Message from Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection stopped with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Version Negotiation Failed with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: Connection established with Controller <y> A.B.C.D
oflow	Openflow Instance <x>: port <z> administratively disabled by controller
oflow	Openflow Instance <x>: port <z> administratively enabled by controller
oflow	ACL table full. Could not add MPLS pop ACL entry for Openflow Flow Table
oflow	ACL table full. Could not add MPLS push ACL entry for Openflow Flow Table
oflow	Openflow Instance <x> Maximum permitted multicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted unicast FDB flows reached
oflow	Openflow Instance <x> Maximum permitted ACL flows reached
oflow	Openflow Instance <x> Maximum permitted MPLS PUSH flows reached
oflow	Openflow Instance <x> Maximum permitted MPLS POP flows reached
oflow	FDB table full. Could not add FDB entry to Openflow Flow Table

Thread	LOG_ALERT Message (continued)
oflow	ACL table full. Could not add ACL entry for Openflow Flow Table
oflow	Openflow statistics cleared for all instances
oflow	Openflow instance <x> Openflow statistics cleared
oflow	Openflow instance <x> Memory not available. Could not modify flow entry in Openflow Flow Table
oflow	Openflow instance <x> Flow Limit reached. Could not perform Flow mod request
oflow	Openflow Instance <x>, change DPID from <0xAAAAA> to <0xBBBBB>
oflow	Memory not available. Could not add flow entry
oflow	Flow Limit reached. Could not add Flow entry to Flow Table
oflow	Openflow dynamic table cleared for all instances
oflow	Openflow dynamic table cleared for instance <x>
oflow	Openflow static table cleared for all instances
oflow	Openflow static table cleared for instance <x>
oflow	Openflow all tables cleared for all instances
oflow	Openflow all tables cleared for instance <x>
OSPF	Interface IP <*IP address*>, Interface State {Down|Loopback|Waiting|P To P|DR|BackupDR|DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down|Attempt|Init|2 Way|ExStart|Exchange|Loading|Full|Loopback|Waiting|P To P|DR|BackupDR|DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
RMON	Event.<*description*>
STP	CIST new root bridge
STP	CIST topology change detected
STP	CIST, interface port <*port*> [moved into|leave from] loop-inconsistent state
STP	CIST, interface port <*port*> [moved into|leave from] root-inconsistent state
STP	STG <*STG*>, interface port <*port*> [moved into|leave from] loop-inconsistent state

Thread	LOG_ALERT Message (continued)
STP	STG <*STG*>, interface port <*port*> [moved into|leave from] root-inconsistent state
STP	STG <*STG*>, new root bridge
STP	STG <*STG*>, topology change detected
STP	Too many BPDUs flooded in VLAN <*VLAN*>. Some of them will be discarded!
SYSTEM	Ingress PVST+ BPDU's spotted from port <*port*>
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <key>
VLAG	vLAG Health check is Down
VLAG	vLAG Health check is Up
VLAG	vLAG ISL is down
VLAG	vLAG ISL is up
VLAG	vLAG on LACP key <*key*> is [up|down]
VLAG	vLAG on portchannel <*trunk ID*> is [up|down]
VRRP	Received <x> virtual routers instead of <y>
VRRP	received errored advertisement from <*IP address*>
VRRP	received incorrect addresses from <*IP address*>
VRRP	received incorrect advertisement interval <interval> from <*IP address*>
VRRP	received incorrect VRRP adver type from <*IP address*>
VRRP	received incorrect VRRP authentication type from <*IP address*>
VRRP	received incorrect VRRP password from <*IP address*>
VRRP	VRRP: received incorrect IP addresses list from <*IP address*>

LOG_CRIT

Thread	LOG_CRIT Message
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private|public key}
SYSTEM	System memory is at <*n*> percent

LOG_ERR

Thread	LOG_ERR Message
CFG	Can't assign a port with same protocol to different VLANs.
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN and management VLAN cannot be private-VLANs.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	ERROR: Cannot enable/disable RMON for Mgmt Port <*port*>
CFG	ERROR: More than <maximum> VLAN(s) in downstream
CFG	Error writing active config to FLASH! Another save is in progress
CFG	Maximum allowed number (30) of Alarm groups have already been created.
CFG	Maximum allowed number (30) of Event groups have already been created.
CFG	Maximum allowed number (5) of History groups have already been created.
CFG	Need to enable port's tag for tagging pvlan.
CFG	Overflow! Port has more than 16 protocols.
CFG	Port is not for this protocol.
CFG	Switch rem port fails when disable {protocol|vlan}.
CFG	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
CFG	WARN: Have not defined protocol type for VLAN <*VLAN*> Protocol <*protocol*>!
DCBX	Duplicate DCBX Application Protocol Sub-TLV detected on port <*port*>
DCBX	Duplicate DCBX Control Sub-TLV detected on port <*port*>
DCBX	Duplicate DCBX PFC Sub-TLV detected on port <*port*>
DCBX	Duplicate DCBX PG Sub-TLV detected on port <*port*>
DCBX	Duplicate DCBX VNIC Sub-TLV detected on port <*port*>
IP6	EXCEPTIONAL CASE Trying to create IP6 Interface after the Ip6Shutdown

Thread	LOG_ERR Message (continued)
IP6	Ip6SetAddr(failed):if=<*interface*>, rc=<*reason code*>
IP6	IPv6 route table full
IP6	ipv6_add_interface_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_nbrcache_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_route_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_vlan_change_immediate: Buffer Non Linear for ip6_cfa_params
LLDP	Error: Port <*port*> has the PVID <*PVID*> that is different from the PVID <*PVID*> configured on the peer
LLDP	Port <*port*>: Cannot add new entry. MSAP database is full!
MGMT	Apply is issued by another user. Try later
MGMT	cannot contact {primary|secondary} DNS server <*IP address*> - {Mgmt|Ext-mgt} port unavailable
MGMT	Critical Error. Failed to add Interface <*interface*>
MGMT	Critical Error. Failed to {add|attach} Loopback Interface <*interface*>
MGMT	Critical Error. Failed to detach Loopback Interface <*interface*>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Pushed {image1|image2} size <*bytes*> bigger than the capacity <*maximum bytes*>.
MGMT	Error: Invalid {image1|image2}
MGMT	Error: Pushed {image1|image2} size <*bytes*> bigger than the capacity <*maximum bytes*>.
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory)
MGMT	Invalide CRC value. Boot image rejected

Thread	LOG_ERR Message (continued)
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later
MGT	You are attempting to load an image that has been corrupted or belongs to another switch type. Please verify you have the correct file for this switch and try again. [Error: Invalid header magic value <*value*>.] Boot image rejected
NTP	unable to listen to NTP port
nsx-gw	VTEP failed to bind logical port to VNI <*VNID*>: port <*port*> link down or removed from VLAN <*VLAN number*>.
nsx-gw	VTEP failed to bind logical port to VNI <*VNID*>: port <*port*> doesn't belong to VLAN <*VLAN number*>.
nsx-gw	VTEP failed to bind logical port to VNI <*VNID*>: VLAN <*VLAN number*> not configured or enabled.
PFC	PFC can be enabled on 2 priorities only - priority 3 and one other priority.
RMON	Maximum {Alarm|Event|History} groups exceeded when trying to add group <*group*> via SNMP
STP	Cannot set "{Hello Time|Max Age|Forward Delay|Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	Error: DHCP Offer was found invalid by ip configuration checking; please see system log for details.
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Not enough memory!
SYSTEM	Port <*port*> disabled. Link params(speed/mode) mismatch with <*trunk name*> <*trunk ID*>
SYSTEM	Port <*port*> disabled. Same LACP admin_key with port "PORT_INT_<*port*> rent link params(speed/mode)"
SYSTEM	{PortChannel|Trunk group} creation failed for {IntPortChannel|PortChannel|Internal Trunk group|Trunk group} <*trunk ID*>. Only <*maximum trunks*> {PortChannels|Trunk groups} supported by hardware.
VRRP	Virtual Router Group is disabled due to no enabled virtual routers.

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user <*username*>.
	System log cleared via SNMP.
HOTLINKS	"Error" is set to "{Active|Standby}"
HOTLINKS	"Learning" is set to "{Active|Standby}"
HOTLINKS	"None" is set to "{Active|Standby}"
HOTLINKS	"Side Max" is set to "{Active|Standby}"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface
MGMT	/* Config changes at <*time*> by <*username*> */ <*config diff*> /* Done */
MGMT	<*username*> ejected from BBI
MGMT	<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
MGMT	boot image changed
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	boot kernel Firmware uploaded.
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser|BBI}
MGMT	Error: Static FDB entry on inexistent VLAN
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image|image1|image2|boot kernel|undefined|SP boot kernel}
MGMT	Firmware downloaded to {invalid image|image1|image2|boot kernel|undefined|SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <*hostname*>:<*filename*>

Thread	LOG_INFO Message (continued)
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1|2 download completed. Now writing to flash.
MGMT	image1|2 downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	image1|2 downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	image1|2 Firmware uploaded.
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	invalid image downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	invalid image Firmware uploaded.
MGMT	NETBOOT: Config successfully downloaded and applied from <*hostname*>:<*filename*>
MGMT	New config set
MGMT	new configuration applied [from BBI|EM|NETBOOT|SCP|SNMP]
MGMT	new configuration saved from {BBI|BladeOS|ISCLI|SNMP}
MGMT	Revert failed: configuration is dumped or modified by another user.
MGMT	scp<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
MGMT	scp<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
MGMT	SP boot kernel download completed. Now writing to flash.

Thread	LOG_INFO Message (continued)
MGMT	SP boot kernel downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	SP boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	SP boot kernel Firmware uploaded.
MGMT	Starting Firmware download for {invalid image|image1|image2|boot kernel|undefined|SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Static FDB entry on invalid VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	Unable to do revert apply. The current configuration is in ISCLI format, it needs to be saved in Lenovo OS format.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	undefined downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	undefined Firmware uploaded.
MGMT	unsaved changes reverted [from BBI|from SNMP]
MGMT	Unsupported GBIC {accepted|refused}
MGMT	user {SNMP user|<*username*>} ejected from BBI
MGMT	Watchdog has been {enabled|disabled}
MGMT	Watchdog timeout interval is now <*seconds*> seconds)
MGMT	Wrong config file type
NETCONF	<*username*> (<*user level*>) connection closed from address via NETCONF over <*connection type*>
NETCONF	<*username*> (<*user level*>) login from host <*IP address*> via NETCONF over <*connection type*>
nsx-gw	Active service node <*IP address*> is down.
nsx-gw	Active service node <*IP address*> is down and no backup service node is up.
nsx-gw	Active service node <*IP address*> is removed.

Thread	LOG_INFO Message (continued)
nsx-gw	Active service node <*IP address*> is removed and no backup service node is up.
nsx-gw	Database syncing is complete.
nsx-gw	OVSDB SSL connection to NVP(ssl:<*IP address*>:<*TCP port*>) is closed.
nsx-gw	OVSDB SSL connection to NVP(ssl:<*IP address*>:<*TCP port*>) is establishing.
nsx-gw	Register database "hardware_vtep" succeed.
nsx-gw	Service node <*IP address*> is active.
nsx-gw	Unregister database "hardware_vtep" succeed.
oflow	OpenFlow <*OpenFlow ID*>: Connection established with controller <*1-4*> <*IP address*>
oflow	Openflow Statistics Cleared
oflow	Openflow Flowtable Cleared
oflow	OpenFlow <*OpenFlow ID*>: Connection lost with controller <*1-4*> <*IP address*>
RMON	RMON {alarm|event|history} index <*ID*> was deleted via SNMP
RMON	SNMP configuration for RMON {alarm|event|history} index <*ID*> applied
SSH	<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
SSH	server key autogen {starts|completes}
SSH	Wrong config file type
SYSTEM	booted version <*version*> from Flash image <*image*>, {active|backup|factory} config block
SYSTEM	FDB Learning {DISABLED|ENABLED} for port <*port*>

Thread	LOG_INFO Message (continued)
SYSTEM	Insert another transceiver or change configuration and manually enable port <*port*>
TFTP	Successfully sent {boot image|image1|mage2} to switch <*MAC adress*>

LOG_NOTICE

Thread	LOG_NOTICE Message
	<*minutes*> {minute|minutes} until scheduled reboot
	ARP table is full.
	Current config successfully tftp'd <*filename*> from <*hostname*>
	Current config successfully tftp'd to <*hostname*>: <*filename*>
	ECMP route configured, Gateway health check enabled
	More than one trunk found for LACP adminkey <*adminkey*>. Static MAC entry <*index*> was added only to trunk <*trunk number*>.
	Number of COSqs has been changed since boot. Save and reset the switch to activate the new configuration.
	Port <*port*> mode is changed to full duplex for 1000 Mbps operation.
	scheduled switch reboot
	switch reset at <*time*> has been canceled
	switch reset scheduled at <*time*>
	Warning: DHCP on IF <*interface*> will be disabled
8021X	Could not create failover checkpoint record for port <*port*>
8021X	Logoff request on port <*port*>
8021X	Port <*port*> {assigned to|removed from} vlan <*VLAN*>
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Type value (<*tunnel type*>); should be 13 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Medium-Type value (<*tunnel type*>); should be 6 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a reserved VLAN and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a non-existent or disabled VLAN, and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has an invalid VLAN id (<*VLAN*>) and cannot be assigned to port <*port*>

Thread	LOG_NOTICE Message (continued)
BGP	bad authentication received / no authentication received / authentication receive error from <*IP address*>
BGP	session established with <*IP address*>
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary|secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
DCBX	Detected DCBX peer on port <*port*>
DCBX	Feature "{DCBX|ETS|PFC|App Proto|VNIC|ETS}" not supported by peer on port <*port*>
DCBX	LLDP [TX &] RX are disabled on port <*port*>
DCBX	LLDP TX is disabled on port <*port*>
DCBX	Not able to detect DCBX peer on port <*port*>
DCBX	Peer on port port stopped responding to DCBX message
FCOE	Failed to create FCOE vlan <*VLAN*>
FCOE	FCF <*MAC address*> has been removed.
FCOE	FCF <*MAC address*> is now operational.
FCOE	FCOE connection between VN_PORT <*MAC address*> and FCF <*MAC address*> {has been established|is down}.
FCOE	FCOE vlan <*VLAN*> created.
FCOE	Port <*port*> has been added to the FCOE vlan <*VLAN*>.
FCOE	VN_PORT <*MAC address*> has been reassigned, the old connection will be deleted.
FCF	FCF configured on vlan <*VLAN Number*>
FCF	FCF disabled on vlan <*VLAN Number*>
HOTLINKS	"Error" is set to "Standby|Active"
HOTLINKS	"Learning" is set to "Standby|Active"
HOTLINKS	"None" is set to "Standby|Active"
HOTLINKS	"Side Max" is set to "Standby|Active"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface
IP	cannot contact multicast router <*IP address*>
IP	Either Route or Arp table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.

Thread	LOG_NOTICE Message (continued)
IP	IGMP - {L3 IPMC|L3 IPv4 Multicas|Backup UP groups|Backup DOWN groups|IGMP groups|IPMC} table is full!
IP	IGMP - V1 timer is running for group <*IP address*>, vlan <*VLAN*>[, port <*port*>] Ignored leave!
IP	L3 table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	mrouter <*IP address*> has been disabled or deleted
IP	multicast router <*IP address*> operational
IP	On Vlan <*VLAN*> IGMP version updated to <*version*>
IP	Received {IGMPv1|IGMPv2} query from <*IP address*>
IP	VLAN <*VLAN*> is not in the igmp relay list. Mrouter <*IP address*> will be down
IP	Warning: DHCP on IF <*interface*> will be disabled
IP	Warning: Enabling dhcp will delete IP interface <*interface*> and IP gateway <*gateway*>'s configurations.
IP	Warning: gateway (<*gateway*>) will be deleted
LACP	All supported trunks already created. Port <*port*> will be disabled by LACP.
LACP	LACP is {up|down} on port <*port*>
LINK	link {down|up} on port <*port*>
LINK	Port <*port*> disabled by PVST Protection
MGMT	<*username*> automatically logged out from BBI because changing of authentication type
MGMT	<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {BBI|Console|Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console|from host <*IP address*>|from BBI}
MGMT	ACL <*old number*> from old configuration file moved to ACL <*new number*> in new configuration file
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed

Thread	LOG_NOTICE Message (continued)
MGMT	Boot profile changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI|TELNET} from host <*IP address*>.
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	Log msg no. <*x*>
MGMT	Membership for Port <*port*> in vlan <*VLAN*> is not effective while the port is assigned with PVID <*PVID*> by 802.1x
MGMT	MGT Gateway <*IP address*> not in the same subnet as the Mgt IP <*IP address*>/<*netmask*>
MGMT	New config set
MGMT	new configuration saved from ISCLI
MGMT	New Management IP Address <*IP address*> configured
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	Password for {oper|operator} changed by {SNMP user|<*username*>}, notifying admin to save.
MGMT	Port <*port*> remains untagged while it is assigned PVID <PVID> by 802.1x
MGMT	QSFP: Port <*port*> changed to {10G|40G}, from {BBI|SNMP|CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary|secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
MGMT	scp<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
MGMT	second syslog host changed to {this host|<*IP address*>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared

Thread	LOG_NOTICE Message (continued)
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host|<*IP address*>}
MGMT	System clock set to <*time*>.
MGMT	System date set to <*date*>.
MGMT	Terminating BBI connection from host <*IP address*>
MGMT	User <*username*> deleted by {SNMP user|<*username*>}.
MGMT	User <*username*> is {deleted|disabled} and will be ejected by {SNMP user|<*username*>}
MGMT	User {oper|operator} is disabled and will be ejected by {SNMP user|<*username*>}.
MGMT	Wrong config file type
NETCONF	<*username*> (<*user level*>) connection closed from address via NETCONF over <*connection type*>
NETCONF	<*username*> (<*user level*>) login from host <*IP address*> via NETCONF over <*connection type*>
NTP	System clock updated
nsx-gw	Disabling NWV mode is in process.....wait.....
nsx-gw	Disabling NWV mode is complete.
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down|Loopback|Waiting|P To P|DR|BackupDR|DR Other|Attempt|Init|2 Way|ExStart|Exchange|Loading|Full}
OSPFV3	Link state database is FULL.Ignoring LSA.
OSPFV3	nbr <*router ID*> changes state from {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL} to {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL}[, Neighbor Down: {Interface down or detached|Dead timer expired}]
OSPFV3	virtual link nbr <*router ID*> changes state from {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL} to {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL}[, Neighbor Down: {Interface down or detached|Dead timer expired}]
SERVER	link {down|up} on port <*port*>
SSH	(remote disconnect msg)
SSH	<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console|from host <*IP address*>}

Thread	LOG_NOTICE Message (continued)
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
SSH	scp<*username*>(<*user type*>) login {on Console|from host <*IP address*>}
SSH	Wrong config file type
SYSTEM	<*SPF name*> TX Fault - <*SFP type*> is DISABLED
SYSTEM	<*SPF name*> UnApproved - <*SFP type*> is DISABLED
SYSTEM	<*SFP type*> inserted at port <*port*> is UNAPPROVED ! Device is DISABLED.
SYSTEM	Address for interface <*interface*> ignored because of mismatch.
SYSTEM	BOOTP Offer (continue): Domain name: <*domain*>
SYSTEM	BOOTP Offer (continue): Host name: <*host*>
SYSTEM	BOOTP Offer (continue): Primary DNS: <*IP address*>, Secondary DNS: <*IP address*>
SYSTEM	Change fibre GIG port <*port*> mode to full duplex
SYSTEM	Change fibre GIG port <*port*> speed to 1000
SYSTEM	Changed ARP entry for IP <*IP address*> to: MAC <MAC address>, Port <*port*>, VLAN <*VLAN*>
SYSTEM	Could not add L2 multicast entry! L2 table is full.
SYSTEM	ECMP route gateway <*IP address*> is {down|up}
SYSTEM	Enable auto negotiation for copper GIG port: <*port*>
SYSTEM	Fan Fault {Detected|Cleared}. Fan <fan number> RPM <RPM value>
SYSTEM	Fan Failure Warning Cleared
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	L2 table is full!
SYSTEM	Mask for interface <*interface*> ignored because of mismatch.
SYSTEM	**** MAX TEMPERATURE (<*temperature*>) ABOVE FAIL THRESH ****
SYSTEM	**** MAX TEMPERATURE (<*temperature*>) ABOVE WARN THRESH ****

Thread	LOG_NOTICE Message (continued)
SYSTEM	**** PLATFORM THERMAL SHUTDOWN ****
SYSTEM	Port <*port*> disabled
SYSTEM	Port <*port*> disabled by BPDU Guard
SYSTEM	Port <*port*> disabled by OAM (unidirectional|TX-RX Loop)
SYSTEM	Port <*port*> disabled by UDLD (unknown|unidirectional|bidirectional|TX-RX loop|neighbor mismatch)
SYSTEM	Port <*port*> disabled due to reason code <*reason code*>
SYSTEM	Power Fault {Cleared|Detected} - <number>
SYSTEM	Power Supply Warning Cleared
SYSTEM	rebooted (<*reason*>)[, administrator logged in] Reason: • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer
SYSTEM	Received BOOTP Offer: IP: <*IP address*>, Mask: <*netmask*>, Broadcast <*IP address*>, GW: <*IP address*>
SYSTEM	Received DHCP Offer: IP: <*IP address*>, Mask: <*netmask*> Broadcast <*IP address*>, GW: <*IP address*>
SYSTEM	server with MAC address <*MAC address*> was {added to|removed from} network
SYSTEM	Static route gateway <*IP address*> is {down|up}
SYSTEM	Warning: Fan Failure
SYSTEM	Warning: Power Supply Disconnected or Failure
SYSTEM	Watchdog threshold changed from <*old value*> to <*new value*> seconds
SYSTEM	Watchdog timer has been enabled
TEAMING	error, action is undefined

Thread	LOG_NOTICE Message (continued)
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
VM	<*IP address*> moved from {port <*port*>|trunk IT <*trunk ID*>} to {port <*port*>|trunk IT <*trunk ID*>}
VM	MAC address <*MAC address*> moved from {port <*port*>|trunk IT <*trunk ID*>} to {port <*port*>|trunk IT <*trunk ID*>}
VM	[(Refresh)] VI server unreachable or certificate invalid.
VM	Virtual Machine with {IP address <*IP address*>|MAC address <*MAC address*>} came online
VM	Virtual Machine with {IP address <*IP address*>|MAC address <*MAC address*>} changed its VLAN to <*new VLAN*>. It was previously in VLAN <*old VLAN*>
VM	Virtual Machine with {IP address <*IP address*>|MAC address <*MAC address*>} is a member of VLAN <*VLAN*>
VM	Virtual Machine with {IP address <*IP address*>|MAC address <*MAC address*>} is not in VLAN <*VLAN*> anymore
VM	[(Refresh)] VM agent command not implemented.
VM	[(Refresh)] VM agent could not be started.
VM	[(Refresh)] VM agent could not login to server.
VM	[(Refresh)] VM agent could not retrieve {host|VM} properties.
VM	[(Refresh)] VM agent encountered a file error.
VM	[(Refresh)] VM agent encountered an IPC error.
VM	[(Refresh)] VM agent file error.
VM	[(Refresh)] VM Agent not active.
VM	[(Refresh)] VM agent operation failed due to a conflict.
VM	[(Refresh)] VM agent operation failed.
VM	[(Refresh)] VM agent operation needs no change.
VM	[(Refresh)] VM agent operation timed out.
VM	[(Refresh)] VM agent protocol error.
VM	VM agent resumed (Refresh).
VM	VM agent resumed (Scan).
VM	[(Refresh)] VM agent timed out and could not be stopped.

Thread	LOG_NOTICE Message (continued)
VM	[(Refresh)] VM agent timed out.
VM	[(Refresh)] VM agent unable to logout from server.
VM	[(Refresh)] VM agent unknown error.
VM	[(Refresh)] VM agent VE limit reached.
VM	[(Refresh)] VM agent: Invalid ID.
VM	VM agent: local table full.
VM	VM MAC <*MAC address*> NOT added to hash table
VM	VM move detected but failed to move network conf
VRRP	virtual router <*IP address*> is now {BACKUP|MASTER}
WEB	<*username*> ejected from BBI
WEB	<*username*> ejected from BBI because username password was changed
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_WARNING

Thread	LOG_WARNING Message
	Static IPMC route group <*group number*> on vlan <*VLAN*> [primary|backup] has been converted to a host route group because IGMP snooping is enabled.
8021X	Authentication session terminated with {Failure|Success} on port <*port*>
8021X	Could not create failover checkpoint record for port <*port*>
8021X	Logoff request on port <*port*>
8021X	Port <*port*> {assigned to|removed from} vlan <*VLAN*>
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Type value (<*tunnel type*>); should be 13 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Medium-Type value (<*tunnel type*>); should be 6 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a reserved VLAN and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a non-existent or disabled VLAN, and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has an invalid VLAN id (<*VLAN*>) and cannot be assigned to port <*port*>
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
CFG	Configured {sip|dip|protocol|tcpl4|udpl4|port|dport} hashing without tcpl4 or udpl4. {sip|dip|protocol|tcpl4|udpl4|port|dport} hashing will be ignored!
CFG	Configured {sip|dip|protocol|tcpl4|udpl4|port|dport} hashing without sport or dport. {sip|dip|protocol|tcpl4|udpl4|port|dport} hashing will be ignored!
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
CFG	Static IPMC route group <*IP address*> on VLAN <*VLAN*> [primary|backup] has been converted to a host route group because IGMP snooping is enabled.

Thread	LOG_WARNING Message (continued)
CFG	Switch cannot support more than 16 protocols simultaneously!
CFG	Trunk hash changed, Dataplane L3 hash includes configured Trunk hash and ECMP hash
CFG	Unfit config exists when protocol-vlan apply.
DCBX	Feature "{DCBX|ETS|PFC|App Proto|VNIC|ETS}" not supported by peer on port <*port*>
ETS	ETS prohibits a PG comprising of PFC and non-PFC traffic. Mixing in the same PG different PFC settings may affect the switch functionality.
HOTLINKS	"Error" is set to "Standby|Active"
HOTLINKS	"Learning" is set to "Standby|Active"
HOTLINKS	"None" is set to "Standby|Active"
HOTLINKS	"Side Max" is set to "Standby|Active"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface
IP	<*IP address*> configured as V<*version*> and received IGMP V{1|2} query
IP	IGMP: Switch Querier {disabled|enabled} on VLAN <*VLAN*>
IP	IGMP: Switch {became|is no longer} a Querier for VLAN <*VLAN*>
IP	IGMP: Switch is [not] elected as Querier for VLAN <*VLAN*>
IP	IGMP: Switch Querier election process started for VLAN <*VLAN*>
IP	IGMP: Switch Querier election type changed for VLAN <*VLAN*>
IP	IGMP: Warning Querier Source-IP is not configured on VLAN <*VLAN*> Queries with Source-IP Zero may be ignored in Querier election process.
IP	IGMP: Warning Snooping is not enabled on VLAN <*VLAN*>, Querier configured only to send queries.
IP	New Multicast router learned on <*IP address*>, VLAN <*VLAN*>, Version {V1|V2|V3}
LLDP	ERROR!!! The request port item <*item*> is invalid
NTP	cannot contact NTP server <*IP address*> - {Mgmt|Ext-mgt} port unavailable
NTP	cannot contact [primary|secondary] NTP server <*IP address*>
FCF	VLAN <*VLAN*>: NPRD VA_RJT Out of order reported
FCF	VLAN <*VLAN*>: NPRD VA_RJT Insufficient resources

Thread	LOG_WARNING Message (continued)
FCF	VLAN <*VLAN*>: NPRD VA_RJT(rc:0x<RC>, expl:0x<RCE>) received.
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Interface <*interface*> failed to renew DHCP Lease.
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled

Appendix B. Getting help and technical assistance

If you need help, service or technical assistance, or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check the Lenovo ServerProven website to make sure that the hardware and software is supported by your product.
- Go to the Lenovo Support portal to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs

- Start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties.

Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and X-Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as total bytes written (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Recycling Information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:

http://www.lenovo.com/recycling

Particulate Contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility..

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication Regulatory Statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic Emission Notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC (until April 19, 2016) and EU Council Directive 2014/30/EU (from April 20, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A equipment according to European Standards harmonized in the Directives in compliance. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

CE Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Germany Class A Statement

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der Klasse A der Norm gemäß Richtlinie.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein

Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EU Richtlinie 2014/30/EU (früher 2004/108/EC), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahrenist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

Japan VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI–A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase).

Korea Communications Commission (KCC) Statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，
可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

W