IBM System Networking RackSwitch™ G8124/G8124E

ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.9

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 IBM *Documentation* CD and the *Warranty Information* document that comes with the product.

Contents

Preface

The *IBM System Networking RackSwitch G8124/G8124E ISCLI Command Reference* describes how to configure and use the IBM N/OS 7.9 software with your RackSwitch G8124 or RackSwitch G8124-E (collectively referred to as G8124 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 *Installation Guide* for your RackSwitch G8124. For details about configuration and operation of your G8124, see the *IBM N/OS 7.9 Application Guide*.

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, Port Trunking, 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, "IBM N/OS System Log Messages," shows a listing of syslog messages.

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

"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` {*<1-12>*|`hash`|`information`} you enter: **show** `portchannel` *<1-12>* 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 {<1-12>|hash|information}` you must enter: **show** `portchannel <1-12>` or show `portchannel` hash or show `portchannel` information

How to Get Help

If you need help, service, or technical assistance, call IBM Technical Support:

US toll free calls: 1-800-414-5268

International calls: 1-408-834-7871

You also can visit our web site at the following address:

`http://www.ibm.com`

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

Chapter 1. ISCLI Basics

Your RackSwitch G8124 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 G8124.

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 IS 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 G8124. Several sub-modes can be accessed from the Global Configuration mode. For more details, see Table 2.

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.

Table 2. lists the ISCLI command modes.

Table 2. ISCLI Command Modes

Command Mode/Prompt	Command used to enter or exit
User EXEC `G8124>`	Default mode, entered automatically on console Exit: `exit` or `logout`
Privileged EXEC `G8124#`	Enter Privileged EXEC mode, from User EXEC mode: `enable` Exit to User EXEC mode: `disable` Quit ISCLI: `exit` or `logout`
Global Configuration `G8124(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: `configure terminal` Exit to Privileged EXEC: `end` or `exit`
Interface IP `G8124(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: `interface ip` *<interface number>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Interface loopback `G8124(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`

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Interface port `G8124(config-if)#`	Enter Port Configuration mode, from Global Configuration mode: `interface port` *<port number or alias>* Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`
Interface PortChannel `G8124(config-PortChannel)#`	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: `interface portchannel` {*<trunk number>*|`lacp` *<key>*} Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`
VLAN `G8124(config-vlan)#`	Enter VLAN Configuration mode, from Global Configuration mode: `vlan` *<VLAN number>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Router OSPF `G8124(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 `G8124(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 `G8124(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`
Router RIP `G8124(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`

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Route Map G8124(config-route-map)#	Enter Route Map Configuration mode, from Global Configuration mode: route-map <*1-64*> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
Router VRRP G8124(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 G8124(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 Router(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 Router(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 G8124(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

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.

`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows:
	
	`ping` *<host name>* | *<IP address>* [`-n` *<tries (0-4294967295)>*] [`-w` *<msec delay (0-4294967295)>*] [`-l` *<length (0/32-65500/2080)>*] [`-s` *<IP source>*] [`-i` *<ttl (1-255)>*] [`-v` *<tos (0-255)>*] [`-f`] [`-t`] [`-ma`|`-mgta`|`-mb`|`-mgtb`|`-d`|`-data`]
	
	Where:
	
	  – `-n`: Sets the number of attempts (optional).
	  – `-w`: Sets the number of milliseconds between attempts (optional).
	  – `-l`: Sets the ping request payload size (optional).
	  – `-s`: Sets the IP source address for the IP packet (optional).
	  – `-i`: Sets the Time to live in the IP header.
	  – `-v`: Sets the Type of Service bits in the IP header.
	  – `-f`: Sets the *don't fragment* bit in the IP header (only for IPv4 addresses).
	  – `-t`: Pings continuously (same as `-n 0`).
	
	By default, the `-ma` or `-mgta` option for management port A is used. To use data ports, specify the `-d` or `-data` option.

Table 3. Description of Global Commands

Command	Action
`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)>*]] `[-ma|-mgta|-mb|-mgtb|-d|-data]` Where *hostname/IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *msec-delay* (optional) is the number of milliseconds to wait for the response. By default, the `-ma` or `-mgta` option for management port A is used. To use data ports, specify the `-d` or `-data` option. As with `ping`, the DNS parameters must be configured if specifying hostnames.
`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>*} [*<port>*] `[-ma|-mgta|-mb|-mgtb|-d|-data]` Where *IP address* or *hostname* specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch. *Port* is the logical Telnet port or service number. By default, the `-ma` or `-mgta` option for management port A is used. To use data ports, specify the `-d` or `-data` option.
`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:

```
# vlan 1,3,4094            (access VLANs 1, 3, and 4094)
# vlan 1-20                (access VLANs 1 through 20)
# vlan 1-5,90-99,4090-4094 (access multiple ranges)
# 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:

```
# 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:

```
G8124(config)# spanning-tree stp 2 bridge hello 2

    or

G8124(config)# sp stp 2 br h 2
```

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 G8124. 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 G8124. 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 G8124. These changes are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset 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/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the G8124. 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.	`user`
Operator	The Operator can make temporary changes that are lost when the switch is rebooted/reset. 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 G8124, 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: – Port alias and number – Port description – Port speed – Duplex mode (half, full, or auto) – Flow control for transmit and receive (no, yes, or both) – Link status (up, down, or disabled) **Command mode:** All For details, see page 101.
`show interface trunk` *<port alias or number>* Displays port status information, including: – Port alias and number – Whether the port uses VLAN Tagging or not – Port VLAN ID (PVID) – Port description – VLAN membership – FDB Learning status – Flooding status For details, see page 101. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each port. For details, see page 103. **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 Table 6, with pointers to where detailed information can be found.

Table 6. System Information Options

Command Syntax and Usage
`show sys-info` Displays system information, including: – System date and time – Switch model name and number – Switch name and location – Time of last boot – MAC address of the switch management processor – IP address of management interface – Hardware version and part number – Software image file and version number – Configuration name – Log-in banner, if one is configured – Internal temperatures – Fan status – Power supply status For details, see page 24. **Command mode:** All
`show logging [severity <0-7>] [reverse]` Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 25. **Command mode:** All
`show access user` Displays configured user names and their status. **Command mode:** All

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 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
`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

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 user` Displays User Security Model (USM) table information. To view the table, see page 16. **Command mode:** All
`show snmp-server v3 view` Displays information about view, subtrees, mask and type of view. To view a sample, see page 17. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 18. **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 19. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 19. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 21. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 22. **Command mode:** All

Table 9. SNMPv3 Information Options (continued)

Command Syntax and Usage
`show snmp-server v3 notify` Displays the Notify table information. To view a sample, see . **Command mode:** All
`show snmp-server v3` Displays all the SNMPv3 information. To view a sample, see . **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 Security 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. IBM N/OS 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.

Table 14. SNMPv3 Community Table Information Parameters (continued)

Field	Description
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
--------------- ---------- -------------------- ------------

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

snmpTargetAddr Table:
Name            Transport Addr                   Port Taglist     Params
--------------- -------------------------------- ---- ------------ -------------

snmpTargetParams Table:
Name                MP Model User Name           Sec Model Sec Level
------------------- -------- -------------------- --------- ------------
```

General System Information

The following command displays system information:

```
show sys-info
```

Command mode: All

```
System Information at 13:41:04 Fri Jan 20, 2011
Time zone: America/Barbados
Daylight Savings Time Status: Disabled


IBM Networking Operating System RackSwitch G8124


Switch has been up for 0 days, 17 hours, 10 minutes and 45 seconds.
Last boot: 20:41:01 Thu Jan 19, 2000 (power cycle)


MAC address: 00:25:03:49:83:00    IP (If 1) address: 0.0.0.0
MGMT-A Port MAC Address: 00:25:03:49:83:ee
MGMT-A Port IP Address (if 127): 12.16.2.45
MGMT-B Port MAC Address: 00:25:03:49:83:ef
MGMT-B Port IP Address (if 128):
Hardware Revision: 18
Board Revision: 2
Switch Serial No: CH4035002U
Hardware Part No: BAC-00045-00        Spare Part No: BAC-00045-00
Manufacturing date: 10/34
Software Version 6.6.0 (FLASH image1), active configuration.


Fans are in Forward AirFlow, Warning at 85 C and Recover at 100 C


Temperature Sensor 1: 28.0 C
Temperature Sensor 2: 33.0 C
Temperature Sensor 3: 37.75 C
Temperature Sensor 4: 42.75 C
Temperature Sensor 5: 36.50 C


Speed of Fan 1:   8231 RPM
Speed of Fan 2:   8294 RPM
Speed of Fan 3:   8256 RPM
Speed of Fan 4:   8231 RPM
Speed of Fan 5:   8411 RPM
Speed of Fan 6:   8530 RPM


State of Power Supply 1:   Off
State of Power Supply 2:   On
```

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

Table 18 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.
 	
    Command mode: All

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

```
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  6:02:12 0.0.0.0 NOTICE  system: link up on management port MGT
Nov  2  6:03:11 172.25.254.19 NOTICE  system: Received DHCP Offer
        IP: 172.25.254.19 Mask: 255.255.0.
        Broadcast 172.25.255.255 GW: 172.25.1.1
Nov  2  6:03:11 0.0.0.0 NOTICE  ip: MGT port default gateway 172.25.1.1 operational
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.

Layer 2 Information

Table 19. Layer 2 Information Commands

Command Syntax and Usage
`show vlag information`   Displays vLAG Information. For details, see page 41.   Command mode: All
`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: – Priority   – Hello interval   – Maximum age value   – Forwarding delay   – Aging time   You can also see the following port-specific STG information: – Port alias and priority   – Cost   – State   **Command mode:** All
`show spanning-tree root`   Displays root bridge ID for every spanning-tree instance and the path cost associated to it.   **Command mode:** All   For details, see page 44.
`show spanning-tree blockedports`   Lists the ports blocked by each STP instance.   **Command mode:** All
`show spanning-tree stp` *\<instance number or range>* `information`   Displays information about a specific Spanning Tree Group.   **Command mode:** All   For details, see page 42.

Table 19. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show spanning-tree mst` *‹instance number or range›* `information` Displays Spanning Tree information for the specified instance. `0` is used for CIST. CIST bridge information includes: – Priority – Hello interval – Maximum age value – Forwarding delay – Root bridge information (priority, MAC address, path cost, root port) CIST port information includes: – Port number and priority – Cost – State For details, see page 45. **Command mode:** All
`show spanning-tree mst configuration` Displays the current MSTP settings. **Command mode:** All
`show portchannel information` Displays the state of each port in the various trunk groups. For details, see page 47. **Command mode:** All
`show vlan` Displays VLAN configuration information for all configured VLANs, including: – VLAN Number – VLAN Name – Status – Port membership of the VLAN For details, see page 47. **Command mode:** All
`show failover trigger` *‹trigger number›* `information` Displays Layer 2 Failover information. For details, see page 34. **Command mode:** All
`show hotlinks information` Displays Hot Links information. For details, see page 36. **Command mode:** All

Table 19. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show lldp information` Displays Link Layer Discovery Protocol (LLDP) information. For details, see page 36. **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

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 16K MAC address entries on the MP per switch.

Table 20. FDB Information Options

Command Syntax and Usage
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 interface port *<port alias or number>* Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table portchannel *<trunk group number>* Displays all FDB entries for a particular trunk group (portchannel). **Command mode:** All
show mac-address-table vlan *<VLAN number>* Displays all FDB entries on a single VLAN. **Command mode:** All
show mac-address-table state {unknown|forward|trunk} Displays all FDB entries for a particular state. **Command mode:** All
show mac-address-table multicast Displays all static multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table static Displays all static unicast MAC entries in the FDB. **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 counters Displays all forwarding database statistics. **Command mode:** All

Table 20. FDB Information Options (continued)

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

FDB Multicast Information

The following commands display FDB multicast information.

Table 21. Multicast FDB Information Options

Command Syntax and Usage

`show mac-address-table multicast address` *<MAC address>* [*<VLAN>*]
 	
    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`

`show mac-address-table multicast interface` *<port number>*   Displays all multicast entries for a particular port.
`show mac-address-table multicast vlan` *<VLAN number>*   Displays all multicast entries on a single VLAN.

`show mac-address-table multicast`
 	
    Displays all Multicast MAC entries in the FDB.
 	
    Command mode: All

Show All FDB Information

The following command displays Forwarding Database information:

`show mac-address-table`

Command mode: All

```
    MAC address      VLAN Port Trnk State Permanent
    ---------------- ---- ---- ---- ----- ---------
    00:04:38:90:54:18   1 4            FWD
    00:09:6b:9b:01:5f   1 13           FWD
    00:09:6b:ca:26:ef 4095 1           FWD
    00:0f:06:ec:3b:00 4095 1           FWD
    00:11:43:c4:79:83   1 4            FWD        P
```

An address that is in the forwarding (`FWD`) state, means that it has been learned by the switch. When in the trunking (`TRK`) state, the port field represents the trunk group 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 .

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the G8124.

Table 22. LACP Information Options

Command Syntax and Usage
show lacp aggregator *<aggregator ID>* Displays detailed information about the LACP aggregator. **Command mode:** All
show interface port *<port alias or number>* lacp information Displays LACP information about the selected port. **Command mode:** All
show lacp information Displays a summary of LACP information. For details, see page 33. **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

Link Aggregation Control Protocol

The following command displays LACP information:

```
show lacp information
```

Command mode: All

```
pport    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 dump includes the following information for each port in the G8124:

- **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 trunk group number.

- **status** Displays the status of LACP on the port (up, down or standby).

- **minlinks** Displays the minimum number of active links in the LACP trunk.

Layer 2 Failover Information

Table 23. Layer 2 Failover Information Options

Command Syntax and Usage

show failover trigger *\<trigger number\>* information
    Displays detailed information about the selected Layer 2 Failover trigger.
    Command mode: All

show failover trigger information
    Displays a summary of Layer 2 Failover information. For details, see page 35.
    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 trunk group, 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 24.   LLDP Information Options

Command Syntax and Usage
show lldp port Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
show lldp transmit Displays information about the LLDP transmit state machine. **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 . **Command mode:** All

Table 24. LLDP Information Options

Command Syntax and Usage
`show lldp remote-device port <port number>` Displays information received from LLDP-capable devices for a specific port. A given list of ports needs to be delimited by ',' and a range of ports delimited by '-'. **Command mode:** All
`show lldp information` Displays all LLDP information. **Command mode:** All

LLDP Remote Device Information

The following command displays LLDP remote device information:

`show lldp remote-device [<1-256>|detail]`

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
----------|-------|---------------------|--------------|---------------------|------
XGE2      | 1     | 34 40 b5 6d ce 00   | 17           |                     | NB
1         | 2     | 00 00 00 00 11 00   | 30           |                     | NB
XGE4      | 3     | 00 e0 00 01 00 00   | 62           |                     | 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 : IBM Networking Operating System RackSwitch™ G8124/G8124E,
IBM Networking OS: version 7.6.0,13 Boot image: version 7.6.0.13
        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

Table 25. UDLD Information Options

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

OAM Discovery Information

Table 26.   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

Table 27. vLAG Information Options

Command Syntax and Usage
`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 portchannel` *<trunk group number>* 　Displays vLAG static trunk group information. 　**Command mode:** All
`show vlag portchannel` *<trunk group number>* `information` 　Displays all vLAG static trunk group information. 　**Command mode**: All
`show vlag isl` 　Displays vLAG Inter-Switch Link (ISL) information. 　**Command mode:** All
`show vlag information` 　Displays all vLAG information. 　**Command mode:** All

vLAG Trunk Information

The following command displays vLAG information for the trunk group:

`show vlag portchannel` *<trunk group number>*

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
```

Spanning Tree Information

The following command displays Spanning Tree information:

```
show spanning-tree stp <instance number or range> 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
              32768      2      20      15      300

   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
MGTA        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. For details see "PVRST Information" on page 45.

The following port-specific information is also displayed:

Table 28. 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), Backup (BKUP).

Table 28. 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.

Spanning Tree Bridge Information

```
------------------------------------------------------------------
Pvst+ compatibility mode enabled

------------------------------------------------------------------
Spanning Tree Group 1: On (RSTP)
VLANs:  1 4095

Current Root:           Path-Cost  Port Hello MaxAge FwdDel
 8000 74:99:75:74:c4:00      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
------------- ---- ---------- ----- ---- -------------------- -------- ----------
5     (pc66)   128      490!+ FWD   DESG 8000-74:99:75:74:c4:00     8083      P2P
```

The following command displays Spanning Tree bridge information:

```
show spanning-tree [vlan <VLAN ID>] bridge
```

Command mode: All

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

Table 29. 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.

Table 29. Bridge Parameter Descriptions (continued)

Parameter	Description
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 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 30. 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 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 <instance number or range> information
```

Command mode: All

```
Mstp Digest: 0xac36177f50283cd4b83821d8ab26de62


Common Internal Spanning Tree:

VLANs MAPPED:  1-4094
VLANs:  1 2 4095

Current Root:            Path-Cost  Port MaxAge FwdDel
 8000 00:11:58:ae:39:00     2026     0    20     15

Cist Regional Root:       Path-Cost
 8000 00:11:58:ae:39:00        0

Parameters:  Priority  MaxAge  FwdDel  Hops
             32768      20      15      20

Port  Prio  Cost      State  Role Designated Bridge     Des Port Hello Type
----- ---- --------- ----- ---- --------------------- -------- ----- ----
1     128   2000!  FWD  ROOT fffe-00:13:0a:4f:7d:d0   8011    2    P2P#
23    128   2000!  DISC ALTN fffe-00:22:00:24:46:00   8012    2    P2P#
MGTA   0       0   FWD *

* = STP turned off for this port.
! = Automatic path cost.
# = PVST Protection enabled for this port.
```

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

Table 31. 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.

Table 31. CIST Parameter Descriptions (continued)

Parameter	Description
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 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 32. 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), Master (MAST), or Unknown (UNK).
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.

Trunk Group Information

The following command displays Trunk Group information:

```
show portchannel information
```

Command mode: All

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

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

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

VLAN Information

Table 33. VLAN Information Options

Command Syntax and Usage

show vlan *<VLAN number>*
 	
    Displays general VLAN information.
    Command mode: All

show vlan private-vlan
 	
    Displays Private VLAN information.
    Command mode: All s

show vlan information
 	
    Displays information about all VLANs, including:
    – VLAN number and name
    – VLAN statistics
    – VLAN creation time
    – Port membership
    – VLAN status (enabled or disabled)
    – Private VLAN status
    – Spanning Tree membership
    – VMAP configuration
    Command mode: All

The following command displays VLAN information:

```
show vlan
```

Command mode: All

```
VLAN            Name                    Status        Ports
----  --------------------------------  ------  ------------------------
1     Default VLAN                        ena   1-20
2     VLAN 2                              dis   21-22
100   VLAN 100                            ena   empty
200   VLAN 200                            ena   empty
300   VLAN 300                            ena   empty
4095  Mgmt VLAN                           ena   MGTA MGTB

Primary      Secondary    Type      Ports
------------ ------------ --------- ---------------
100          200          isolated  14
100          300          community 12
```

```
VLAN            Name                    Status        Ports
----  --------------------------------  ------  ------------------------
1     Default VLAN                        ena   1-16 19-24
2     VLAN 2                              ena   17 18
100   VLAN 100                            ena   empty
200   VLAN 200                            ena   empty
300   VLAN 300                            ena   empty
4095  Mgmt VLAN                           ena   MGTA MGTB

Private-VLAN   Type      Mapped-To          Status      Ports
------------ --------- ------------------  ---------- --------------------
100          primary   200 300             ena        empty
200          isolated  100                 ena        empty
300          community 100                 ena        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
• Private VLAN information (if available)

Layer 3 Information

Table 34. Layer 3 Information Commands

Command Syntax and Usage
`show ip route` Displays all routes configured on the switch. For details, see page 53. **Command mode:** All
`show arp` Displays Address Resolution Protocol (ARP) information. For details, see page 54. **Command mode:** All
`show ip bgp information [IPv4 address] [IPv4 mask]` Displays Border Gateway Protocol (BGP) information. For details, see page 58. **Command mode**: All
`show ip ospf information` Displays the OSPF information. For details, see page 59. **Command mode**: All
`show ipv6 ospf information` Displays OSPFv3 information. For more OSPFv3 information options, see page 64. **Command mode**: All
`show ip rip interface` Displays RIP user's configuration. For details, see page 68. **Command mode**: All
`show ipv6 route` Displays IPv6 routing information. For more information options, see page 69. **Command mode**: All
`show ipv6 neighbors` Displays IPv6 Neighbor Cache information. For more information options, see page 70. **Command mode**: All
`show ipv6 prefix` Displays IPv6 Neighbor Discovery prefix information. For details, see page 71. **Command mode**: All
`show ip ecmp` Displays ECMP static route information. For details, see page 71. **Command mode**: All

Table 34. Layer 3 Information Commands (continued)

Command Syntax and Usage
`show ip igmp groups` Displays IGMP Information. For more IGMP information options, see . **Command mode**: All
`show ipv6 mld groups` Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see . **Command mode**: All
`show ip vrrp information` Displays VRRP information. For details, see . **Command mode:** All
`show interface ip` Displays IP interface Information. For details, see . **Command mode:** All
`show ipv6 interface` *<interface number>* Displays IPv6 interface information. For details, see . **Command mode:** All
`show ipv6 pmtu` [*<destination IPv6 address>*] Displays IPv6 Path MTU information. For details, see . **Command mode:** All
`show ip interface brief` Displays IP Information. For details, see . IP information, includes: – IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. – Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status – IP forwarding settings, network filter settings, route map settings **Command mode:** All
`show ikev2` Displays IKEv2 information. For more information options, see . **Command mode:** All
`show ipsec manual-policy` Displays information about manual key management policy for IP security. For more information options, see . **Command mode:** All

Table 34. Layer 3 Information Commands (continued)

Command Syntax and Usage
`show ip dhcp snooping binding` Displays DHCP Snooping information. For details, see . **Command mode:** All
`show ip pim component [<`*`1-2`*`>]` Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see . **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 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 35. Route Information Options

Command Syntax and Usage
`show ip route address` *<IP address>* Displays a single route by destination IP address. **Command mode:** All
`show ip route gateway` *<IP address>* Displays routes to a single gateway. **Command mode:** All
`show ip route type {indirect`|`direct`|`local`|`broadcast`|`martian`|`multicast}` Displays routes of a single type. For a description of IP routing types, see Table 36 on page 53. **Command mode:** All
`show ip route tag {fixed`|`static`|`addr`|`rip`|`ospf`|`bgp`|`broadcast`|`martian`|`multicast}` Displays routes of a single tag. For a description of IP routing tags, see Table 37 on page 53. **Command mode:** All
`show ip route interface` *<interface number>* Displays routes on a single interface. **Command mode:** All
`show ip route ecmphash` Displays the current ECMP hashing mechanism. **Command mode:** All
`show ip route static` Displays static routes configured on the switch. **Command mode:** All
`show ip route` Displays all routes configured in the switch. **Command mode:** All For more information, see page 53.

Show All IP Route Information

The following command displays IP route information:

```
show ip route
```

Command mode: All

```
Status code: * - best
   Destination      Mask            Gateway          Type       Tag       Metr If
   --------------- --------------- --------------- --------- --------- ---- --
 * 0.0.0.0          0.0.0.0         172.31.1.1       indirect  static       1
 * 12.0.0.0         255.0.0.0       0.0.0.0          martian   martian
 * 12.31.0.0        255.255.0.0     172.31.36.139    direct    fixed        1
 * 12.31.36.139     255.255.255.255 172.31.36.139    local     addr         1
 * 12.31.255.255    255.255.255.255 172.31.255.255   broadcast broadcast    1
 * 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 36. 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 37. 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 G8124.
addr	The address belongs to one of the switch's IP interfaces.
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)

Table 37. IP Routing Tag Parameters (continued)

Parameter	Description
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 39 on page 55), VLAN and port for the address, and port referencing information.

Table 38. ARP Information Options

Command Syntax and Usage
`show arp find` *<IP address>*   Displays a single ARP entry by IP address.   **Command mode:** All
`show arp interface port` *<port alias or number>*   Displays the ARP entries on a single port.   **Command mode:** All
`show arp vlan` *<VLAN number>*   Displays the ARP entries on a single VLAN.   **Command mode:** All
`show arp`   Displays all ARP entries. including: – IP address and MAC address of each entry   – Address status flag   – The VLAN and port to which the address belongs   – The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)   For more information, see page 55.   **Command mode:** All
`show arp reply`   Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.   **Command mode:** All

ARP Address List Information

The following command displays owned ARP address list information:

```
show arp reply
```

Command mode: All

```
    IP address        IP mask         MAC address      VLAN Pass-Up
 --------------- --------------- ----------------- ---- -----
 12.31.36.139    255.255.255.255 00:13:0a:4f:7e:30    1
 205.178.50.1    255.255.255.255 00:70:cf:03:20:06    1
 205.178.18.64   255.255.255.255 00:70:cf:03:20:05    1
```

Show All ARP Entry Information

The following command displays ARP information:

```
show arp
```

Command mode: All

```
    IP address    Flags    MAC address     VLAN Age Port
 --------------- ----- ----------------- ---- --- ----
 10.100.130.1          00:0e:40:99:cc:5d    1 276 19
 10.100.130.12   P     00:22:00:d5:a8:00    1
```

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

The `Flags` field is interpreted as follows:

Table 39. 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.

BGP Information

Table 40. BGP Peer Information Options

Command Syntax and Usage
`show ip bgp neighbor information` Displays BGP peer information. See page 56 for a sample output. **Command mode:** All
`show ip bgp neighbor group` Displays BGP group information. See page 57 for a sample output. **Command mode:** All
`show ip bgp neighbor summary` Displays peer summary information such as AS, message received, message sent, up/down, state. See page 58 for a sample output. **Command mode:** All
`show ip bgp neighbor <`*neighbor number*`> redistribution` Displays BGP neighbor redistribution. **Command mode:** All
`show ip bgp neighbor <`*neighbor number*`> routes` Displays BGP peer routes. **Command mode:** All
`show ip bgp information` Displays the BGP routing table. See page 58 for a sample output. **Command mode:** All
`show ip bgp neighbor advertised-routes` Displays all BGP advertised routes to all neighbors. **Command mode**: All
`show ip bgp neighbor <`*1-96*`> advertised-routes` Displays all BGP advertised routes to a specific neighbor. **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>]
```

Command mode: All

```
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Mask            Next Hop        Metr 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 13.0.0.0 is filtered out by rrmap; or, a loop detected.
```

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

OSPF Information

Table 41. OSPF Information Options

Command Syntax and Usage
`show ip ospf general-information` Displays general OSPF information. See page 60 for a sample output. **Command mode:** All
`show ip ospf area information` Displays area information for all areas. **Command mode:** All
`show ip ospf area` *‹area index›* Displays area information for a particular area index. **Command mode:** All
`show interface ip {`*‹interface number›*`} ospf` Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See page 61 for a sample output. **Command mode:** All
`show interface loopback {`*‹interface number›*`}` Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces. See page 61 for a sample output. **Command mode:** All
`show ip ospf area-virtual-link information` Displays information about all the configured virtual links. **Command mode:** All
`show ip ospf neighbor` Displays the status of all the current neighbors. **Command mode:** All
`show ip ospf summary-range` *‹area index›* Displays the list of summary ranges belonging to non-NSSA areas. **Command mode:** All
`show ip ospf summary-range-nssa` *‹area index›* Displays the list of summary ranges belonging to NSSA areas. **Command mode:** All

Table 41. OSPF Information Options (continued)

Command Syntax and Usage

```
show ip ospf routes
```
Displays OSPF routing table. See for a sample output.

Command mode: All

```
show ip ospf information
```
Displays the OSPF information.

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

```
show ip ospf interface loopback
```

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 Database Information

Table 42. OSPF Database Information Options

Command Syntax and Usage
`show ip ospf database advertising-router` *\<router ID>* Takes advertising router as a parameter. Displays all the Link State Advertisements (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 asbr-summary`
`[advertising-router` *\<router ID>*`|link-state-id` *\<A.B.C.D>*`|self]`
 	
Displays ASBR summary LSAs. The usage of this command is as follows:
 	
a. `asbr-summary advertising-router 20.1.1.1` displays ASBR summary LSAs having the advertising router 20.1.1.1.
 	
b. `asbr-summary link-state-id 10.1.1.1` displays ASBR summary LSAs having the link state ID 10.1.1.1.
 	
c. `asbr-summary self` displays the self advertised ASBR summary LSAs.
 	
d. `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: a. Number of LSAs of each type in each area. b. Total number of LSAs for each area. c. Total number of LSAs for each LSA type for all areas combined. d. 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>*`|`
`link-state-id` *\<A.B.C.D>*`|self]`
 	
Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs.
 	
Command mode: All

`show ip ospf database network [advertising-router` *\<router ID>*`|`
`link-state-id` *\<A.B.C.D>*`|self]`
 	
Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database.
 	
Command mode: All

`show ip ospf database nssa` Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. **Command mode:** All

Table 42. OSPF Database Information Options (continued)

Command Syntax and Usage

`show ip ospf database router [advertising-router <router ID>|`
`   link-state-id <A.B.C.D>|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>|link-state-id <A.B.C.D>|self]`
 	
Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs.
 	
Command mode: All

`show ip ospf database` Displays all the LSAs. **Command mode:** All

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
```

OSPFv3 Information

Table 43.   OSPFv3 Information Options

Command Syntax and Usage
`show ipv6 ospf area` *<area index (0-2)>* Displays the area information
`show ipv6 ospf areas` Displays the OSPFv3 Area Table. **Command mode:** All
`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 66. **Command mode:** All
`show ipv6 ospf area-virtual-link information` Displays information about all the configured virtual links. **Command mode:** All
`show ipv6 ospf neighbor` *<nbr router-id (A.B.C.D)>* 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 host information` Displays OSPFv3 host configuration information. **Command mode:** All
`show ipv6 ospf request-list` *<nbr router-id (A.B.C.D)>* 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 (A.B.C.D)>* 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 summary-prefix` *<area index (0-2)>* Displays the OSPFv3 external summary-address configuration information. **Command mode:** All

Table 43. OSPFv3 Information Options (continued)

Command Syntax and Usage
`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 area-range information` Displays OSPFv3 summary ranges. **Command mode:** All
`show ipv6 ospf routes` Displays OSPFv3 routing table. To view a sample display, see . **Command mode:** All
`show ipv6 ospf border-routers` Displays OSPFv3 routes to an ABR or ASBR. **Command mode:** All
`show ipv6 ospf information` Displays all OSPFv3 information. To view a sample display, see . **Command mode:** All

OSPFv3 Information Dump

```
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

Table 44. OSPFv3 Database Information Options

Command Syntax and Usage
`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

Table 44.   OSPFv3 Database Information Options (continued)

Command Syntax and Usage

`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 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

`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 [detail|hex]`
 	
    Displays all the LSAs.
 	
    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

Table 45.   Routing Information Protocol Options

Command Syntax and Usage

`show ip rip routes`
 	
   Displays RIP routes.
 	
   Command mode: All
 	
   For more information, see page 68.

`show ip rip interface` *<interface number>*
 	
   Displays RIP user's configuration.
 	
   Command mode: All
 	
   For more information, see page 68.

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

Table 46 describes the IPv6 Routing information options.

Table 46. IPv6 Routing Information Options

Command Syntax and Usage
show ipv6 route address *<IPv6 address>*   Displays a single route by destination IP address.
show ipv6 route gateway *<default gateway address>*   Displays routes to a single gateway.
show ipv6 route type {connected|static|ospf}   Displays routes of a single type. For a description of IP routing types, see Table 36 on page 53.
show ipv6 route interface *<interface number>*   Displays routes on a single interface.
show ipv6 route summary   Displays a summary of IPv6 routing information, including inactive routes.
show ipv6 route   Displays all IPv6 routing information. For more information, see page 69.

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
, E - Ext-Management Gateway
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

Table 47. IPv6 Neighbor Cache Information Options

Command Syntax and Usage

`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 vlan` *\<VLAN number\>*
 	
    Displays IPv6 Neighbor Cache entries on a single VLAN.
 	
    Command mode: All

`show ipv6 neighbors static`
 	
    Displays static IPv6 Neighbor Cache entries.
 	
    Command mode: All

`show ipv6 neighbors counters`
 	
    Displays statistics for all entries.
 	
    Command mode: All

`show ipv6 neighbors`
 	
    Displays all IPv6 Neighbor Cache entries. For more information, see .
 	
    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 Multicast Group Information

Table 48.   IGMP Multicast Group Information Commands

Command Syntax and Usage
`show ip igmp querier vlan` *<VLAN number or range>* Displays IGMP Querier information for a particular VLAN. For details, see [page 74](#). **Command mode:** All
`show ip igmp querier port` *<port alias>* Displays IGMP Querier information for a particular port. **Command mode:** All
`show ip igmp snoop` Displays IGMP Snooping information. **Command mode:** All
`show ip igmp mrouter information` Displays IGMP Multicast Router information. For details, see [page 74](#). **Command mode:** All
`show ip igmp mrouter vlan` *<VLAN number>* Displays IGMP Multicast Router information for the specified VLAN. **Command mode:** All
`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 filtering` Displays current IGMP Filtering parameters. **Command mode:** All
`show ip igmp profile` *<1-16>* Displays information about the current IGMP filter. **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 vlan` *<VLAN number>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All

Table 48. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage
`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` *\<trunk number\>* Displays all IGMP multicast groups on a single trunk group. **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` Displays information for all multicast groups. For details, see . **Command mode:** All
`show ip igmp ipmcgrp` Displays information for all IPMC groups. For details, see . **Command mode:** All
`show ip igmp counters` Displays IGMP counters for all VLANs. **Command mode:** All
`show ip igmp counters` *\<VLAN number\>* Displays IGMP counters for a specific VLAN. **Command mode:** All

IGMP Querier Information

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

`show ip igmp querier vlan` *<VLAN number or range>*

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

Table 49 describes the commands used to view MLD information.

Table 49. 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 number>* Displays MLD groups on a single interface port. **Command mode:** All
show ipv6 mld groups portchannel *<trunk group number>* Displays groups on a single port channel. **Command mode:** All
show ipv6 mld groups vlan *<vlan number>* Displays groups on a single VLAN. **Command mode:** All
show ipv6 mld mrouter Displays all MLD Mrouter ports. See page 78 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 50. 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 G8124 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 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 127.31.35.5    255.255.0.0  172.31.255.255,  vlan 1,    up
  2: IP6 2002:0:0:0:0:0:0:5/64 ,                       vlan 1,    up
        fe80::213:aff:fe4f:7c01
  3: IP6 3003:0:0:0:0:0:0:5/64 ,                       vlan 2,    up
        fe80::213:aff:fe4f:7c02

127: IP6 10:90:90:0:0:0:0:97/64 ,                      vlan 4095, DOWN
128: IP4 10.90.90.97   255.255.255.0  10.90.90.255,   vlan 4095, up
```

For each interface, the following information is displayed:

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

Note: If routing is enabled using the "`no switchport`" command in Interface Port mode, this command also displays IP interfaces configured on physical ports as well as LACP and LAGs.

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, 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:
Flood unregistered IPMC: ena
  AS number 0

Interface information:
  1: IP4 192.168.1.253   255.255.255.0   192.168.1.255,   vlan 100, up
 99: IP4 192.168.99.100  255.255.255.0   192.168.99.255,  vlan 99, DOWN
127: IP4 172.25.101.222  255.255.0.0     172.25.255.255,  vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  3: 172.25.1.1,      up  active

Default IP6 gateway information:

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
 ...
         MGTA       No           none
         MGTB       No           none
Current IP forwarding settings: ON, dirbr disabled, ICMPv6 redirect disabled
Current network filter settings:
  none
Current route map settings:
RIP is disabled.
OSPF is disabled.
OSPFv3 is disabled.
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 51. IKEv2 Information Commands

Command Syntax and Usage
`show ikev2` Displays all IKEv2 information. See 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-2

Local preshare key:         ibm123

IKEv2 choose IPv6 address as ID type
No SAD entries.
```

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(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.
- Security Association Database (SAD) entries, if applicable.

IP Security Information

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

Table 52. IPsec Information Commands

Command Syntax and Usage
`show ipsec sa` Displays all security association information. **Command mode:** All
`show ipsec spd` Displays all security policy information. **Command mode:** All
`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 87 for sample output. **Command mode:** All
`show ipsec transform-set <1-10>` Displays IPsec transform set information. **Command mode:** All
`show ipsec traffic-selector <1-10>` Displays IPsec traffic selector information. **Command mode:** All
`[no] debug sec all` Enables or disables all IP security debug messages. **Command mode:** Global configuration
`[no] debug sec crypto` Enables or disables cryptographic debug messages. **Command mode:** Global configuration
`[no] debug sec ike` Enables or disables IKEv2 debug messages. **Command mode:** Global configuration
`[no] debug sec ipsec` Enables or disables IPsec debug messages. **Command mode:** Global configuration

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 Binding Table Information

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
0e:f7:5b:6a:74:d8  75.179.93.39    86337          Static   232  1


Total number of bindings: 8
```

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

Table 53. PIM Information Options

Command Syntax and Usage
`show ip pim bsr [<`*component ID*`>]` 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 90. **Command mode:** All
`show ip pim counters` Displays PIM statistics for all interfaces. **Command mode:** All
`show ip pim interface [<`*interface number*`>|detail|loopback|port` `<`*port number*`>]` Displays PIM interface information. To view sample output, see page 91. **Command mode:** All
`show ip pim neighbor [<`*interface number*`>|port <`*port number*`>]` Displays PIM neighbor information. To view sample output, see page 91. **Command mode:** All
`show ip pim neighbor-filters` Displays information about PIM neighbor filters. **Command mode:** All

`show ip pim mroute [<`*component ID*`>|count|flags|`
`group <`*multicast group address*`>|`
`interface {<`*interface number*`>|port <`*port number*`>}`
`source <`*multicast source address*`>]`
 	
Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see page 92.
 	
Command mode: All

`show ip pim rp-candidate [<`*component ID*`>]` 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

Table 53. PIM Information Options (continued)

Command Syntax and Usage
`show ip pim rp-static [<`*component ID*`>]` Displays a list of the static Rendezvous Points configured. **Command mode:** All
`show ip pim elected-rp [group <`*multicast group address*`>]` Displays a list of the elected Rendezvous Points. **Command mode:** All

PIM Component Information

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

`show ip pim component [<`*component ID*`>]`

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

Table 54. PIM Multicast Route Information Options

Command Syntax and Usage
show ip pim mroute [<*component ID*>] Displays PIM multicast routes for the selected component. **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: – S: Shortest Path Tree (SPT) bit – R: Rendezvous Point Tree (RPT) bit – 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 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
show ip pim mroute count Displays a count of PIM multicast routes of each type. **Command mode:** All
show ip pim mroute Displays information about all PIM multicast routes. **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

Table 55. QoS information Options

Command Syntax and Usage
show qos transmit-queue   Displays mapping of 802.1p value to Class of Service queue number, and COS queue weight value.   **Command mode:** All
show qos transmit-queue information   Displays all 802.1p information.   **Command mode:** All   For details, see .
show qos random-detect   Displays WRED and ECN information.   **Command mode:** All   For details, see .

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
...
```

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

Table 56. 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 57. 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

Table 58. ACL Information Options

Command Syntax and Usage
show access-control list *<ACL number>* Displays ACL list information. For details, see page 96. **Command mode:** All
show access-control list6 *<ACL number>* Displays IPv6 ACL list information. **Command mode:** All
show access-control vmap *<VMAP number>* Displays VMAP information. **Command mode:** All

Access Control List Information

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

show access-control list *<ACL number>*

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 59. 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.

Table 59. ACL List Parameter Descriptions

Parameter	Description
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
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.

RMON Information Commands

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

Table 60. RMON Information Options

Command Syntax and Usage
`show rmon history` Displays RMON History information. For details, see page 98. **Command mode:** All
`show rmon alarm` Displays RMON Alarm information. For details, see page 99. **Command mode:** All
`show rmon event` Displays RMON Event information. For details, see page 100. **Command mode:** All
`show rmon` Displays all RMON information. **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 61. 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 62. 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: – abs—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. – 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: – falling—alarm is triggered when a falling threshold is crossed. – rising—alarm is triggered when a rising threshold is crossed. – 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 62. 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 63. 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, 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

```
----------------------------------------------------------------------
Alias   Port   Speed   Duplex   Flow Ctrl     Link    Description
-------  ----   -----   --------  --TX-----RX--   ------   -------------
1        1      10000   full      no    no        down    1
60       60     10000   full      no    no        down    60
61       61     10000   full      no    no        up      61
62       62     10000   full      no    no        up      62
63       63     10000   full      no    no        up      63

MGTA     25     100     full      yes   yes       up
MGTB     26     10      half      yes   yes       down
```

Use this command to display link status information about each port on the G8124, including:

- Port alias and port number
- Port description
- Port speed and Duplex mode (half, full, 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

```
Alias Port Tag RMON Lrn Fld PVID   DESCRIPTION    VLAN(s)
          Trk             NVLAN
----- ---- --- ---- --- --- -----  -------------- --------------------
1     1    n   d    e   e   1                      1
2     2    n   d    e   e   1                      1
3     3    n   d    e   e   1                      1
4     4    n   d    e   e   1                      1
5     5    n   d    e   e   1                      1
...
MGTA  25   n   d    e   e   4095                   4095
MGTB  26   n   d    e   e   4095                   4095

* = PVID/Native-VLAN is tagged.

Trk  = Trunk mode
NVLAN = Native-VLAN
```

Port information includes:

- Port alias and 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 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      Device  TX  RXSig TXuW  RXuW  TXFlt Volts DegsC Laser  Approval
-------- ------- --- ----- ----- ----- ----- ----- ----- ------ ----------
Port  1  SR SFP+ Ena LINK  570.9 661.8 no    3.30 40.5  850nm  Approved
   Detail ->   Vendor: Blade Network
               Part:   BN-CKM-SP-SR
               Date:   080528
               S/N:    AD0822ER07R
Port  2  SR SFP+ Ena LINK  623.5 462.9 no    3.34 40.5  850nm  Approved
   Detail ->   Vendor: Blade Network
               Part:   BN-CKM-SP-SR
               Date:   101104
               S/N:    BNTAJJ031H
Port  3  SR SFP+ Ena LINK  562.2 520.5 no    3.31 37.5  850nm  Approved
   Detail ->   Vendor: Blade Network
               Part:   BN-CKM-SP-SR
               Date:   090623
               S/N:    AD0926ER015
Port  4  SR SFP+ Ena Down  567.0   0.1 no    3.31 34.5  850nm  Approved
   Detail ->   Vendor: Blade Network
               Part:   BN-CKM-SP-SR
               Date:   100505
               S/N:    AA1018A3RC3
Port  5  1m DAC  N/A LINK  ----.- ----.- -N/A- -.-- --.-  -N/A-  Approved
   Detail ->   Vendor: BLADE NETWORKS
               Part:   BN-SP-CBL-1M
               Date:   091106
               S/N:    APF09450020579
Port  6  1m DAC  N/A LINK  ----.- ----.- -N/A- -.-- --.-  -N/A-  Approved
   Detail ->   Vendor: BLADE NETWORKS
               Part:   BN-SP-CBL-1M
               Date:   091111
               S/N:    APF09460021270
...
```

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

- Name identifies the port number and media type
- TX enable/disable
- RXlos: Receive Loss of Signal indicator
- TXFlt: Transmission Fault indicator
- Volts: Power usage, in volts
- DegsC: Temperature, in degrees centigrade
- TXuW: Transmit power, in micro-watts
- RXuW: Receive power, in micro-watts
- Media/Transceiver type (LX, LR, SX, SR)
- Laser wavelength, in nanometers
- Approval status

Virtual Machines Information

The following command display information about Virtual Machines (VMs).

Table 64.   Virtual Machines Information Options

Command Syntax and Usage

show virt port *<port alias or number>*
     Displays Virtual Machine information for the selected port.
     Command mode: All

show virt vm
     Displays all Virtual Machine information.
     Command mode: All

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: 8
* indicates VMware ESX Service Console Interface
+ indicates VMware ESX/ESXi VMKernel or Management Interface
```

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

- 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
- State of the Virtual Machine (~ indicates the VM is inactive/idle)

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
```

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 65. VMware Information Options

Command Syntax and Usage

show virt vmware hosts
     Displays a list of VMware hosts.
     Command mode: All

show virt vmware showhost *<host UUID>|<host IP address>|<host name>*
     Displays detailed information about a specific VMware host.
     Command mode: All

show virt vmware showvm *<VM UUID>|<VM IP address>|<VM name>*
     Displays detailed information about a specific Virtual Machine (VM).
     Command mode: All

show virt vmware vms
     Displays a the names of all VMware VMs.
     Command mode: All

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.

vNIC Information

The following commands display information about Virtual NICs (vNICs).

Table 66. vNIC Information Options

Command Syntax and Usage

`show vnic vnic`
 	
    Displays information about each vNIC.
 	
    Command mode: All

`show vnic vnicgroup`
 	
    Displays information about each vNIC Group, including:
    – Status (enabled or disabled)
    – VLAN assigned to the vNIC Group
    – Uplink Failover status (enabled or disabled)
    – Link status for each vNIC (up, down, or disabled)
    – Port link status for each port associated with the vNIC Group (up, down, or disabled)
 	
    Command mode: All

`show vnic information-dump`
 	
    Displays all vNIC information.
 	
    Command mode: All

Virtual NIC (vNIC) Information

The following command displays Virtual NIC (vNIC) information:

```
show vnic vnic
```

Command mode: All

```
vNIC      vNICGroup  Vlan    MaxBandwidth  Link
--------  ---------  ------  ------------  ---------
1.1       1          3001    30            up
1.2       2          3002    20            up
1.3       3          3003    15            up
1.4       4          3004    10            up
6.1       10         1234    15            up
6.2       #          *       5             up
6.3       #          *       40            up
6.4       #          *       40            up
7.1       1          3001    40            up
7.2       2          3002    24            up
7.3       3          3003    23            up
8.1       1          3001    25            down
8.2       2          3002    25            down
...


# = Not added to any vNIC group
* = Not added to any vNIC group or no vlan set for its vNIC group
```

vNIC information includes the following for each vNIC:
- vNIC ID
- vNIC Group that contains the vNIC
- VLAN assigned to the vNIC Group
- Maximum bandwidth allocated to the vNIC
- MAC address of the vNIC, if applicable
- Link status (up, down, or disabled)

vNIC Group Information

The following command displays vNIC Group information:

```
show vnic vnicgroup
```

Command mode: All

```
vNIC Group  1: enabled
----------------------------------------------
VLAN       : 3001
Failover   : enabled

vNIC       Link
---------- ---------
1.1        up
7.1        up
8.1        down
9.1        up
10.1       up

Port       Link
---------- ---------
2          up

UplinkPort Link
---------- ---------
10         up
```

vNIC Group information includes the following for each vNIC Group:
- Status (enabled or disabled)
- VLAN assigned to the vNIC Group
- Uplink Failover status (enabled or disabled)
- Link status for each vNIC (up, down, or disabled)
- Port link status for each port associated with the vNIC Group (up, down, or disabled)

•

Converged Enhanced Ethernet Information

Table 67 describes the Converged Enhanced Ethernet (CEE) information options.

Table 67. CEE Information Options

Command Syntax and Usage

`show cee information`
   Displays all CEE information
   Command mode: All

DCBX Information

Table 68 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 68. DCBX Information Options

Command Syntax and Usage

`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 111.
   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 112.
   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 113.
   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 114.
   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 115.
   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

DCBX Control Information

The following command displays DCBX Control information:

```
show cee information dcbx port <port range> control
```

Command mode: All

```
Alias Port OperStatus OperVer MaxVer SeqNo AckNo
----- ---- ---------- ------- ------ ----- -----
    1  1      enabled    0       0      0     0
    2  2      enabled    0       0      4     2
    3  3      enabled    0       0      0     0
    4  4      enabled    0       0      1     1
...
   20 20      enabled    0       0      0     0
   21 21      enabled    0       0      0     0
   22 22      enabled    0       0      0     0
   23 23      enabled    0       0      0     0
   24 24      enabled    0       0      0     0
```

DCBX Control information includes the following:

- Port alias and 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, number, or range>* feature

Command mode: All

```
DCBX Port Feature State-machine Info
====================================
Alias Port Type    AdmState Will Advrt OpVer MxVer PrWill SeqNo Err OperMode Syncd
----- ---- ------- -------- ---- ----- ----- ----- ------ ----- --- -------- ---
    1  1   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
    2  2   ETS     enabled  No   Yes   0     0     Yes    4     No  enabled  Yes
    3  3   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
    4  4   ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
    5  5   ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
    6  6   ETS     disabled No   Yes   0     0     No     0     No  disabled No
    7  7   ETS     disabled No   Yes   0     0     No     0     No  disabled No
    8  8   ETS     disabled No   Yes   0     0     No     0     No  disabled No
    9  9   ETS     disabled No   Yes   0     0     No     0     No  disabled No
   10 10   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
...
```

The following table describes the DCBX Feature information.

Table 69. DCBX Feature Information Fields

Parameter	Description
Alias	Displays each port's alias.
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.
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
====================================================
Alias Port Priority PgIdDes PgIdOper PgIdPeer
----- ---- -------- ------- -------- --------
   2  2    0        PGID0   PGID0    PGID0
   2  2    1        PGID0   PGID0    PGID0
   2  2    2        PGID0   PGID0    PGID0
   2  2    3        PGID1   PGID0    PGID0
   2  2    4        PGID2   PGID0    PGID0
   2  2    5        PGID2   PGID0    PGID0
   2  2    6        PGID2   PGID0    PGID0
   2  2    7        PGID2   PGID0    PGID0

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

The following table describes the DCBX ETS information.

Table 70. DCBX Feature Information Fields

Parameter	Description
DCBX Port Priority Group - Priority Allocation Table	
Alias	Displays each port's alias
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 70. DCBX Feature Information Fields (continued)

Parameter	Description
DCBX Port Priority Group - Bandwidth Allocation Table	
Alias	Displays each port's alias
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
=====================================
Alias Port Priority EnableDesr EnableOper EnablePeer
----- ---- -------- ---------- ---------- ----------
   2   2    0       disabled   disabled   disabled
   2   2    1       disabled   disabled   disabled
   2   2    2       disabled   disabled   disabled
   2   2    3       enabled    disabled   disabled
   2   2    4       disabled   disabled   disabled
   2   2    5       disabled   disabled   disabled
   2   2    6       disabled   disabled   disabled
   2   2    7       disabled   disabled   disabled
```

DCBX PFC information includes the following:
- Port alias and 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

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

FIP Snooping Priority Information
=================================
Protocol ID          : 0x8914
Selector Field       : 0
Organizationally Unique ID: 0x1b21

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

The following table describes the DCBX Application Protocol information.

Table 71. 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
Alias	Port alias
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

Table 72 describes the Enhanced Transmission Selection (ETS) information options

Table 72. 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

Table 73 describes the Priority Flow Control (PFC) information options.

Table 73. PFC Information Options

Command Syntax and Usage

show cee port *<port number or range of ports>* pfc
 	
    Displays PFC information.
 	
    Command mode: All

show cee port *<port number or range of ports>* pfc priority *<0-7>*
 	
    Displays PFC information.
 	
    Command mode: All

show cee port *<port number or range of ports>* pfc information
 	
    Displays PFC information.
 	
    Command mode: All

The following command displays PFC information:

show cee port *<port number or range of ports>* 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

Table 74 describes the FIP Snooping information options.

Table 74. FIP Snooping Information Options

Command Syntax and Usage
`show fcoe information` Displays all current FCoE information. **Command mode:** All
`show fcoe fips port <port alias, number, or range> 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 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 vlan` Displays VLAN information. **Command mode:** All

The following command displays FIP Snooping information for the selected port:

```
show fcoe fips port <port alias or number> information
```

Command mode: All

```
FIP Snooping on port INT2:
This port has been configured to automatically detect FCF.
 It has currently detected to have 0 FCF connecting to it.

FIPS ACLs configured on this port:
SMAC 00:c0:dd:13:9b:6f, action deny.
SMAC 00:c0:dd:13:9b:70, action deny.
SMAC 00:c0:dd:13:9b:6d, action deny.
SMAC 00:c0:dd:13:9b:6e, action deny.
DMAC 00:c0:dd:13:9b:6f, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:70, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6d, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6e, ethertype 0x8914, action permit.
SMAC 0e:fc:00:01:0a:00, DMAC 00:c0:dd:13:9b:6d, ethertype 0x8906, vlan 1002, action
permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

```
show fcoe fips port information
```

Command mode: All

```
    FCF MAC         Port    Vlan
----------------------------------
00:05:73:ce:96:67   46      1002
   VN_PORT MAC          FCF MAC          Port    Vlan
-------------------------------------------------------
0e:fc:00:44:04:03   00:05:73:ce:96:67    18      1002
0e:fc:00:44:04:02   00:05:73:ce:96:67    19      1002
0e:fc:00:44:04:04   00:05:73:ce:96:67    21      1002

FIP Snooping on port 1:
This port has been configured to automatically detect FCF.
 It has currently detected to have 0 FCF connecting to it.

FIPS ACLs configured on this port:
SMAC 00:05:73:ce:96:67, action deny.
DMAC 00:05:73:ce:96:67, ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

- Fibre Channel Forwarding (FCF) mode
- Number of FCF links connected to the port
- List of FIP Snooping ACLs assigned to the port

FIP Snooping FCoE Forwarder Information

The following command shows FCoE forwarder (FCF) information that has been learned (detected) by the switch:

```
show fcoe fips fcf
```

Command mode: All

```
Total number of FCFs detected: 0
```

Command mode: All

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 75. Statistics Commands

Command Syntax and Usage
`show layer3 counters` Displays Layer 3 statistics. **Command mode:** All
`show snmp-server counters` **Command mode:** All Displays SNMP statistics. See page 193 for sample output.
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. **Command mode:** All See page 197 for a sample output and a description of NTP Statistics.
`clear mp-counters` Clears all MP-related statistics. **Command mode:** Privileged EXEC
`clear cpu` Clears all CPU utilization statistics. **Command mode:** Privileged EXEC
`clear interface port <`*port number*`> counters` Clears all statistics for the specified port. **Command mode:** All
`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. **Command mode:** All For details, see page 199.

Port Statistics

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

Table 76. Port Statistics Commands

Command Syntax and Usage
show ip bootp-relay counters interface *<port alias or number>* Displays BOOTP relay statistics for the port. **Command mode:** All See page 125 for sample output.
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. **Command mode:** All See page 126 for sample output.
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>* ethernet-counters Displays Ethernet ("dot3") statistics for the port. **Command mode:** All See page 127 for sample output.
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 130 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>* link-counters Displays link statistics for the port. See page 131 for sample output. **Command mode:** All

Table 76. Port Statistics Commands (continued)

Command Syntax and Usage
show interface port *<port alias or number>* rmon-counters   Displays Remote Monitoring (RMON) statistics for the port. See page 132 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
clear interface port *<port alias or number>* counters   Clears all statistics for the port.   **Command mode:** Privileged EXEC
clear counters   Clears statistics for all ports.   **Command mode:** Privileged EXEC

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
```

Table 77. 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
```

Table 78. 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 78. 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 78. 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
Discards:                      0                     0
Errors:                        0                 21187
```

Table 79. 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.
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.

Table 79. Interface Statistics of a Port (continued)

Statistics	Description
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.

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
```

Table 80. 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 EXT2:

etherStatsDropEvents:              NA
etherStatsOctets:                   0
etherStatsPkts:                     0
etherStatsBroadcastPkts:            0
etherStatsMulticastPkts:            0
etherStatsCRCAlignErrors:           0
etherStatsUndersizePkts:            0
etherStatsOversizePkts:             0
etherStatsFragments:               NA
etherStatsJabbers:                  0
etherStatsCollisions:               0
etherStatsPkts64Octets:             0
etherStatsPkts65to127Octets:        0
etherStatsPkts128to255Octets:       0
etherStatsPkts256to511Octets:       0
etherStatsPkts512to1023Octets:      0
etherStatsPkts1024to1518Octets:     0
```

Table 81. 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 81. 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).
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).

Table 81. RMON Statistics of a Port (continued)

Statistics	Description
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).

Trunk Group Statistics

Table 82. Trunk Group Statistics Commands

Command Syntax and Usage

show interface portchannel *<trunk group number>* interface-counters
    Displays interface statistics for the trunk group.
    Command mode: All

clear interface portchannel *<trunk group number>* counters
    Clears all the statistics on the selected trunk group.
    Command mode: All except User EXEC

Layer 2 Statistics

Table 83. Layer 2 Statistics Commands

Command Syntax and Usage
`show mac-address-table counters` Displays FDB statistics. See page 136 for sample output. **Command mode:** All
`clear mac-address-table counters` Clears FDB statistics. **Command mode:** Privileged EXEC
`show interface port` *‹port alias or number›* `lacp counters` Displays Link Aggregation Control Protocol (LACP) statistics. See page 136 for sample output. **Command mode:** All
`clear interface port` *‹port alias or number›* `lacp counters` Clears Link Aggregation Control Protocol (LACP) statistics. **Command mode:** Privileged EXEC
`show hotlinks counters` Displays Hot Links statistics. See page 137 for sample output. **Command mode:** All
`clear hotlinks` Clears all Hot Links statistics. **Command mode:** Privileged EXEC
`show interface port` *‹port alias or number›* `lldp counters` Displays LLDP statistics. See page 138 for sample output. **Command mode:** All
`show oam counters` Displays OAM statistics. See page 139 for sample output. **Command mode:** All
`show vlag statistics` Displays all vLAG statistics. See page 140 for sample output. **Command mode:** All

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 84. 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 85. 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.

Table 85. LACP Statistics

Statistic	Description
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 86. 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 87. 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.

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 88. vLAG Statistics Options

Command Syntax and Usage
show vlag isl-statistics   Displays vLAG ISL statistics for the selected port. See page 140 for sample output.   **Command mode:** All
clear vlag statistics   Clears all vLAG statistics.   **Command mode:** Privileged EXEC
show vlag statistics   Displays all vLAG statistics. See page 140 for sample output.   **Command mode:** All

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).

vLAG Statistics

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 89. VLAG Statistics

Statistic	Description
Role Election	Total number of vLAG PDUs sent for role elections.
System Info	Total number of vLAG PDUs sent for getting system information.
Peer Instance Enable	Total number of vLAG PDUs sent for enabling peer instance.

Table 89. VLAG Statistics (continued)

Statistic	Description
Peer Instance Disable	Total number of vLAG PDUs sent for disabling peer instance.
FDB Dynamic Add	Total number of vLAG PDUs sent for addition of FDB dynamic entry.
FDB Dynamic Del	Total number of vLAG PDUs sent for deletion of FDB dynamic entry.
FDB Req Confirm	Total number of vLAG PDUs requests confirmed.
FDB Inactive Add	Total number of vLAG PDUs sent for addition of FDB inactive entry.
FDB Inactive Del	Total number of vLAG PDUs sent for deletion of FDB inactive entry.
Health Check	Total number of vLAG PDUs sent for health checks.
ISL Hello	Total number of vLAG PDUs sent for ISL hello.
Other	Total number of vLAG PDUs sent for other reasons.
Unknown	Total number of vLAG PDUs sent for unknown operations.

Layer 3 Statistics

Table 90. Layer 3 Statistics Commands

Command Syntax and Usage

`show ip counters`
 	
    Displays IP statistics. See page 146 for sample output.
 	
    Command mode: All

`clear ip counters`
 	
    Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics.
 	
    Command mode: Privileged EXEC

`show ipv6 counters`
 	
    Displays IPv6 statistics. See page 148 for sample output.
 	
    Command mode: All

`clear ipv6 counters`
 	
    Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics.
 	
    Command mode: Privileged EXEC

`show ip route counters`
 	
    Displays route statistics. See page 152 for sample output.
 	
    Command mode: All

`show ip arp counters`
 	
    Displays Address Resolution Protocol (ARP) statistics. See page 154 for sample output.
 	
    Command mode: All

`show ip dns counters`
 	
    Displays Domain Name System (DNS) statistics. See page 154 for sample output.
 	
    Command mode: All

`show ip icmp counters`
 	
    Displays ICMP statistics. See page 155 for sample output.
 	
    Command mode: All

`show ip tcp counters`
 	
    Displays TCP statistics. See page 157 for sample output.
 	
    Command mode: All

`show ip udp counters`
 	
    Displays UDP statistics. See page 158 for sample output.
 	
    Command mode: All

Table 90. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`show ip ospf counters`   Displays OSPF statistics. See for sample output.   **Command mode:** All
`show ipv6 ospf counters`   Displays OSPFv3 statistics. See for sample output.   **Command mode:** All
`show ip igmp counters`   Displays IGMP statistics. See for sample output.   **Command mode:** All
`show ip igmp port` *<port alias>* `counter`   Displays port IGMP statistics.   **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 groups that are registered on the switch.   **Command mode:** All
`show ip vrrp counters`   When virtual routers are configured, you can display the protocol statistics for VRRP. See for sample output.   **Command mode:** All
`show ip pim counters`   Displays PIM statistics for all configured PIM interfaces. See for sample output.   **Command mode:** All
`show ip pim mroute count`   Displays statistics of various multicast entry types.   **Command mode:** All
`show ip pim interface` {*<interface number>*|`loopback`|`port` *<port number>*} `counters`   Displays PIM statistics for the selected interface.   **Command mode:** All

Table 90. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`show ip rip counters` Displays Routing Information Protocol (RIP) statistics. See for sample output. **Command mode:** All
`clear ip arp counters` Clears Address Resolution Protocol (ARP) 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 tcp counters` Clears Transmission Control Protocol (TCP) statistics. **Command mode:** Privileged EXEC
`clear ip udp counters` Clears User Datagram Protocol (UDP) statistics. **Command mode:** Privileged EXEC
`clear ip igmp [<`*VLAN number*`>] counters` Clears IGMP statistics. **Command mode:** Privileged EXEC
`clear ip vrrp counters` Clears VRRP 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*`>|loopback|port <`*port number*`>} counters` Clears PIM statistics on the selected interface. **Command mode**: Privileged EXEC
`clear ip counters` Clears IP statistics. Use this command with caution as it will delete all the IP statistics. **Command mode:** Privileged EXEC

Table 90. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`clear ip rip counters` Clears Routing Information Protocol (RIP) statistics. **Command mode:** Privileged EXEC
`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
`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

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 91. 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 91. 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
```

Table 92. describes the IPv6 statistics.

Table 92. 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 92. 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.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).

Table 92. IPv6 Statistics (continued)

Statistic	Description
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 93. 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.
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.

Table 93. ICMP Statistics

Statistic	Description
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.

Table 94. describes the UDP statistics.

Table 94. 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
```

Table 95. 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 Routing Information Protocol (RIP) routes in the route table.
Current OSPF routes	Total number of OSPF routes in the route table.
Current BGP routes	Total number of Border Gateway Protocol 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.

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
```

Table 96. 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 `clear` option to delete all IPv6 route statistics.

ARP statistics

The following command displays Address Resolution Protocol statistics.

```
show ip arp counters
```

Command mode: All

```
ARP statistics:
arpEntriesCur:            3  arpEntriesHighWater:         4
arpEntriesMax:         2048
```

Table 97. 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.

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
```

Table 98. 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
```

Table 99. 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.
icmpInTimestampReps	The number of ICMP Timestamp `Reply` messages received.

Table 99. ICMP Statistics (continued)

Statistic	Description
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
```

Table 100. 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.
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.

Table 100. TCP Statistics (continued)

Statistic	Description
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
```

Table 101. 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
```

Table 102. 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
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.

Table 102. IGMP Statistics (continued)

Statistic	Description
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

Table 103 describes the commands used to view MLD statistics.

Table 103. MLD Statistics Commands

Command Syntax and Usage
`show ipv6 mld counters` Displays MLD statistics. See page 162 for sample output. **Command mode:** All
`show ipv6 mld groups counters` Displays total number of MLD entries. **Command mode:** All
`show ipv6 mld interface` Displays information for all MLD interfaces. **Command mode:** All
`show ipv6 mld interface` *<interface number>* Displays MLD interface statistics for the specified interface. **Command mode:** All
`show ipv6 mld interface` *<interface number>* `counters` Displays total number of MLD entries on the interface. **Command mode:** All
`show ipv6 mld interface counters` Displays total number of MLD entries. **Command mode:** All
`clear ipv6 mld counters` Clears MLD counters. **Command mode:** All except User Exec
`clear ipv6 mld dynamic` Clears all dynamic MLD tables. **Command mode:** All except User Exec
`clear ipv6 mld groups` Clears dynamic MLD registered group tables. **Command mode:** All except User Exec
`clear ipv6 mld mrouter` Clears dynamic MLD Mrouter group tables. **Command mode:** All except User 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              RxErrors
------------     --------------------  --------------------  --------------------
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              RxErrors
------------     --------------------  --------------------  --------------------

MLD interface packet statistics for interface 3:
MLD msg type          Received            Sent              RxErrors
------------     --------------------  --------------------  --------------------
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 104. 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

Table 105. OSPF Statistics Commands

Command Syntax and Usage

`show ip ospf counters`
    Displays OSPF statistics. See page 165 for sample output.
    Command mode: All

`show ip ospf area counters`
    Displays OSPF area statistics.
    Command mode: All

`show ip ospf interface [`*<interface number>*`] counters`
    Displays OSPF interface statistics.
    Command mode: All

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
```

Table 106. 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.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.

Table 106. OSPF General Statistics (continued)

Statistic	Description
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.
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.

Table 106. OSPF General Statistics (continued)

Statistic	Description
bad sequence	The sum total number of Database Description packets which have been received that either: a. Has an unexpected DD sequence number b. Unexpectedly has the init bit set c. 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 106. 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

Table 107. OSPFv3 Statistics Commands

Command Syntax and Usage
`show ipv6 ospf counters` Displays OSPFv3 statistics. **Command mode:** All
`show ipv6 ospf area counters` Displays OSPFv3 area statistics. **Command mode:** All
`show ipv6 ospf interface` [*<interface number>*] `counters` Displays OSPFv3 interface statistics. **Command mode:** All

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.

Table 108. 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.
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.

Table 108. OSPFv3 General Statistics (continued)

Statistics	Description
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.
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.

Table 108. OSPFv3 General Statistics (continued)

Statistics	Description
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 G8124 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
```

Table 109. 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
```

Table 110. 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

Table 111. 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.

Management Processor Statistics

Table 112. Management Processor Statistics Commands

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 179. **Command mode:** All
`show mp tcp-block` Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 186. **Command mode:** All
`show mp udp-block` Displays all UDP control blocks that are in use. To view a sample output, see page 187. **Command mode:** All
`show processes cpu` Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 187. **Command mode:** All

MP Packet Statistics

Table 113. Packet Statistics Commands

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 179. **Command mode:** All
`show mp packet clear` Clears all packet statistics and logs. **Command mode:** All
`show mp packet logs` Displays a log of all packets received by the CPU. **Command mode:** All
`show mp packet last` *<number of logs>* Displays a list of the most recent packets received by the CPU. **Command mode:** All

Table 113. Packet Statistics Commands (continued)

Command Syntax and Usage
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 182. **Command mode:** All
show mp packet dump Displays all packet statistics and logs. **Command mode:** All

MP Packet Statistics

The following command displays MP packet statistics:

```
show mp packet counters
```

Command mode: All

```
 CPU packet statistics at 16:57:24 Sat Apr  5, 2011

 Packets received by CPU:
 ------------------------
 Total packets:          7642 (7642 since bootup)
 BPDUs:                  5599
 Cisco packets:             0
 ARP packets:            1732
 IPv4 packets:            113
 IPv6 packets:              0
 LLDP PDUs:               198
 Other:                     0

Packet Buffer Statistics:
-------------------------
 allocs:        14311
 frees:         14311
 failures:          0
 dropped:           0

 small packet buffers:
 ---------------------
   current:               0
   max:                2048
   threshold:           512
   hi-watermark:          1
   hi-water time:  14:59:46 Sat Apr  5, 2011

 medium packet buffers:
 ----------------------
   current:               0
   max:                2048
   threshold:           512
   hi-watermark:          1
   hi-water time:  14:59:49 Sat Apr  5, 2011

 jumbo packet buffers:
 ---------------------
   current:               0
   max:                   4
   hi-watermark:          0

 pkt_hdr statistics:
 ---------------------
 current      :             0
 max          :          3072
 hi-watermark :           208
```

Table 114. 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.
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.

Table 114. Packet Statistics (continued)

Statistics	Description
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.
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.

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 Table 115.

Table 115. 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 rarp` Displays only Reverse-ARP packets. **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 lacp` Displays only LACP PDUs 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 ipv4` Displays only IPv4 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 pim` Displays only PIM packets logged. **Command mode:** All

Table 115. Packet Log Parsing Options (continued)

Command Syntax and Usage

`show mp packet parse rx|tx icmp`
 	
    Displays only ICMP packets logged.
 	
    Command mode: All

`show mp packet parse rx|tx tcp`
 	
    Displays only TCP packets 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

`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

`show mp packet parse rx|tx telnet`
 	
    Displays only TELNET 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 udp`
 	
    Displays only UDP packets 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 ntp`
 	
    Displays only NTP packets logged.
 	
    Command mode: All

Table 115. Packet Log Parsing Options (continued)

Command Syntax and Usage
`show mp packet parse rx|tx radius` Displays only RADIUS 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 tftp` Displays only TFTP 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 ipv6` Displays only IPv6 packets logged. **Command mode:** All
`show mp packet parse rx|tx rip` Displays only RIP packets logged. **Command mode:** All
`show mp packet parse rx|tx ospf` Displays only OSPF 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 lldp` Displays only LLDP PDUs logged. **Command mode:** All
`show mp packet parse rx|tx vlan <VLAN_number>` Displays only logged packets with the specified VLAN. **Command mode:** All
`show mp packet parse rx|tx port <port_number>` Displays only logged packets with the specified port. **Command mode:** All

Table 115. Packet Log Parsing Options (continued)

Command Syntax and Usage
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 ip-addr *<IPv4_address>* Displays only logged packets with the specified IPv4 address. **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 raw Displays raw packet buffer in addition to headers. **Command mode:** All
show mp packet parse rx|tx mgmtsock Displays only packets logged from management ports. **Command mode:** All

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

```
Data Ports:
----------------------------------------------------------------
All TCP allocated control blocks:
14835bd8:  0.0.0.0                               0 <=>
           172.31.38.107                        80 listen MGT up
147c6eb8:  0:0:0:0:0:0:0:0                        0 <=>
           0:0:0:0:0:0:0:0                       80  listen
147c6d68:  0.0.0.0                               0 <=>
           0.0.0.0                               80  listen
14823918:  172.31.37.42                      55866 <=>
           172.31.38.107                        23 established 0 ??
11af2394:  0.0.0.0                               0 <=>
           172.31.38.107                        23 listen MGT up
147e6808:  0.0.0.0                               0 <=>
           0.0.0.0                               23  listen
147e66b8:  0:0:0:0:0:0:0:0                        0 <=>
           0:0:0:0:0:0:0:0                       23  listen
147e6568:  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      0 172.31.38.107:http      *:*                   LISTEN
tcp       0      0 172.31.38.107:telnet    *:*                   LISTEN
tcp       0      0 *:11000                 *:*                   LISTEN
tcp       0   1274 172.31.38.107:telnet    172.31.37.42:55866    ESTABLISHED
```

Table 116. 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 MGT1 up	State

UDP Statistics

The following command displays UDP statistics:

```
show mp udp-block
```

Command mode: All

```
Data Ports:
------------------------------------------------------------------
All UDP allocated control blocks:
   68:  listen
  161:  listen
  500:  listen


Mgmt Ports:
------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address        Foreign Address       State
udp        0      0 172.31.38.107:snmp    *:*
udp        0      0 172.31.38.107:bootpc  *:*


172.31.35.1        67 <=> 172.31.38.107     68  accept  MGTA  up

172.25.160.114  40391 <=> 172.31.38.107    161  accept  MGTA  up
```

CPU Statistics

The following commands display 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 thread util  : 100% by  58 (I2C ) at 11:31:32 Sat Mar 10, 2012
----------------------------------------------------------------------
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      0.00%    0.01%    0.38%    0.08%     running
   6     TNET      0.00%    0.00%    0.00%    0.00%     idle
...
 123     PBR       0.00%    0.00%    0.00%    0.00%     idle
 124     HIST      0.00%    0.00%    0.00%    0.00%     idle
 126     NORM      0.00%    0.00%    0.00%    0.00%     idle
 127     DONE      0.00%    0.00%    0.00%    0.00%     idle
----------------------------------------------------------------------
```

Table 117. 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
---------------------------------------------
 17 (IP  )  98% at  22:17:24 Mon Feb 20, 2012
 59 (LACP)   9% at  22:17:33 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:34 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:36 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:40 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:45 Mon Feb 20, 2012
110 (ETMR)  17% at  22:17:47 Mon Feb 20, 2012
110 (ETMR)  18% at  22:17:49 Mon Feb 20, 2012
110 (ETMR)  25% at  22:20:28 Mon Feb 20, 2012
110 (ETMR)  26% at  22:39:08 Mon Feb 20, 2012
 37 (SNMP)  28% at  22:46:20 Mon Feb 20, 2012
 94 (PROX)  57% at  23:29:36 Mon Feb 20, 2012
 94 (PROX)  63% at  23:29:37 Mon Feb 20, 2012
 94 (PROX)  63% at  23:29:39 Mon Feb 20, 2012
 58 (I2C )  64% at  16:21:54 Tue Feb 21, 2012
  5 (CONS)  86% at  18:41:54 Tue Feb 21, 2012
 58 (I2C )  88% at  18:41:55 Tue Feb 21, 2012
 58 (I2C )  88% at  21:29:41 Sat Feb 25, 2012
 58 (I2C )  98% at  12:04:59 Tue Feb 28, 2012
 58 (I2C ) 100% at  11:31:32 Sat Mar 10, 2012
---------------------------------------------
```

QoS Statistics

Table 118. 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.   **Command mode:** All
show qos protocol-packet-control queue-counters   Displays the total number of packets received by each queue.   **Command mode:** All
clear qos protocol-packet-control protocol-counters *\<packet type\>*   Clears packet queue statistics for the selected packet type.   **Command mode:** All
clear qos protocol-packet-control queue-counters *\<queue number\>*   Clears packet queue statistics for the selected queue.   **Command mode:** All
clear qos protocol-packet-control all   Clears all packet queue statistics.   **Command mode:** All

Access Control List Statistics

Table 119. ACL Statistics Commands

Command Syntax and Usage
`show access-control list` *‹ACL number›* `counters` Displays the Access Control List statistics for a specific ACL. **Command mode:** All
`show access-control list6` *‹ACL number›* `counters` Displays the IPv6 ACL statistics for a specific ACL. **Command mode:** All
`show access-control macl` *‹MACL number›* `counters` Displays the ACL statistics for a specific management ACL (MACL). **Command mode:** All
`show access-control counters` Displays all ACL statistics. **Command mode:** All
`show access-control vmap {`*‹vmap number›*`} counters` Displays VLAN Map statistics for the selected VMAP. For a sample display, see . **Command mode:** All
`clear access-control list {`*‹ACL number›*`|all} counters` Clears ACL statistics. **Command mode:** Privileged EXEC
`clear access-control list6 {`*‹ACL number›*`|all} counters` Clears IPv6 ACL statistics. **Command mode:** Privileged EXEC
`clear access-control macl {`*‹ACL number›*`|all} counters` Clears Management ACL (MACL) statistics. **Command mode:** Privileged EXEC
`clear access-control vmap {`*‹VMAP number›*`} counters` Clears VLAN Map statistics. **Command mode:** Privileged EXEC

Table 119. ACL Statistics Commands (continued)

Command Syntax and Usage

`show access-control meter <meter number> counters`
 	
    Displays ACL meter statistics.
 	
    Command mode: All

`clear access-control meter <meter number> counters`
 	
    Clears ACL meter 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 {<vmap number>} counters`

Command mode: All

```
Hits for VMAP 1:            57515
```

FCoE Initialization Protocol Snooping Statistics

The following command displays FCOE Initialization Protocol (FIP) Snooping statistics:

```
show fcoe counters
```

Command mode: All

```
FCOE statistics:
FCFAdded:                   5   FCFRemoved:                 1
FCOEAdded:                 81   FCOERemoved:               24
```

Fiber Channel over Ethernet (FCoE) statistics are described in the following table:

Table 120. FCoE Statistics (/stats/fcoe)

Statistic	Description
FCFAdded	Total number of FCoE Forwarders (FCF) added.
FCFRemoved	Total number of FCoE Forwarders (FCF) removed.
FCOEAdded	Total number of FCoE connections added.
FCOERemoved	Total number of FCoE connections removed.

The total can accumulate over several FCoE sessions, until the statistics are cleared.

The following command clears FCoE statistics:

```
clear fcoe counters
```

Command mode: Privileged EXEC

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
```

Table 121. 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 121. 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 121. 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 121. 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

IBM N/OS 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
```

Table 122. 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 122. 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
```

Table 123. 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

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 124. General Configuration Commands

Command Syntax and Usage
`show running-config` Dumps current configuration to a script file. For details, see page 430. **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
`copy running-config backup-config` Copy the current (running) configuration from switch memory to the `backup-config` partition. For details, see page 431. **Command mode:** Privileged EXEC
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the `startup-config` partition. **Command mode:** Privileged EXEC
`write memory` Copy the current (running) configuration from switch memory to the `active-config` partition. **Command mode:** Privileged EXEC
`copy running-config {ftp|tftp|sftp}[data-port|mgt-port]` Backs up current configuration to a file on the selected FTP/TFTP/SFTP server. **Command mode:** Privileged EXEC

Table 124. General Configuration Commands

Command Syntax and Usage
`copy {ftp|tftp|sftp} running-config [data-port|mgt-port]` Restores current configuration from a FTP/TFTP/SFTP server. **Command mode:** Privileged EXEC For details, see .
`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: – `ca-cert`: Certificate Authority root certificate – `host-key`: host private key – `host-cert`: host public key – `public-key`: host public key **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 G8124 reloads the settings after a reset.

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:

```
G8124(config)# copy running-config startup-config
```

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 reset, see .

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.ele

Table 125. System Configuration Options

Command Syntax and Usage
`system date` *\<yyyy\> \<mm\> \<dd\>*   Prompts the user for the system date. The date retains its value when the switch is reset.   **Command mode:** Global configuration
`system time` *\<hh\>*:*\<mm\>*:*\<ss\>*   Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.   **Command mode:** Global configuration
`system timezone`   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.   **Command mode:** Global configuration
`[no] system daylight`   Disables or enables 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
`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
`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

Table 125. System Configuration Options (continued)

Command Syntax and Usage

`no line vty`
 	
    Sets `line vty length` to the default value of 28.
 	
    Command mode: Global configuration

`system idle` *<0-60>*
 	
    Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle.
 	
    Command mode: Global configuration

`system notice` *<maximum 1024 character multi-line login notice>* *<'.' to end>*
 	
    Displays a login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines.
 	
    Command mode: Global configuration

[no] `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] `hostname` *<character string>*
 	
    Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).
 	
    Command mode: Global configuration

[no] `system bootp`
 	
    Enables or disables the use of BOOTP. If you enable BOOTP, the switch will query its BOOTP server for all of the switch IP parameters. The default setting is `enabled`.
 	
    Command mode: Global configuration

[no] `system default-ip {data|mgta|mgtb}`
 	
    Enables or disables default IP address on interface 1 and required management interfaces, if any. The default setting is `enabled`.
 	
    Command mode: Global configuration

[no] `system dhcp {mgta|mgtb}`
 	
    Enables or disables Dynamic Host Control Protocol for setting the IP address on the scted interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`.
 	
    Command mode: Global configuration

Table 125. System Configuration Options (continued)

Command Syntax and Usage
[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. **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] 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. Setting is applied and device is reset to default factory configuration after reboot. By default, this setting is disabled. **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

CPU Rate Limit Configuration

Use this menu to set limits on inbound packets of various types, which allows you to tune and prioritize traffic received by the switch's management processor.

Table 126. CPU Rate Limit Configuration Options

Command Syntax and Usage
system cpu-rate-limit arp *<1-100>* Configures the CPU rate limit on inbound ARP packets, in megabits per second. **Command mode:** Global configuration
system cpu-rate-limit bpdu *<1-100>* Configures the CPU rate limit on inbound BPDU packets (such as STP and LACP), in megabits per second. **Command mode:** Global configuration

Table 126. CPU Rate Limit Configuration Options (continued)

Command Syntax and Usage
`system cpu-rate-limit control-packet` *<1-100>* Configures the CPU rate limit on inbound control packets (such as IGMP and DHCP), in megabits per second. **Command mode:** Global configuration
`system cpu-rate-limit other` *<1-100>* Configures the CPU rate limit on inbound other packet types (such as data and ICMP), in megabits per second. **Command mode:** Global configuration
`show system cpu-rate-limit` Displays the current CPU Rate Limit configuration. **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 127. Error Disable Configuration Options

Command Syntax and Usage
`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. **Note**: When you change the timeout value, all current error-recovery timers are reset. **Command mode:** Global configuration
`errdisable recovery` Globally enables 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
`no errdisable recovery` Globally disables error-recovery for error-disabled ports; `errdisable recovery` is disabled globally by default. **Command mode:** All
`show errdisable` Displays the current system Error Disable configuration. **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 128. Link Flap Dampening Configuration Options

Command Syntax and Usage
`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
`errdisable link-flap enable` Enables Link Flap Dampening. **Command mode**: Global configuration
`no errdisable link-flap enable` Disables Link Flap Dampening. **Command mode**: Global configuration
`show errdisable link-flap` Displays the current Link Flap Dampening parameters. **Command mode**: All

System Host Log Configuration

Table 129. Host Log Configuration Options

Command Syntax and Usage
[no] `logging host` *<1-2>* `address` *<IP address>* Sets the IP address of the first or second syslog host. **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 is 7, which means log all severity levels. **Command mode:** Global configuration
`logging host` *<1-2>* `facility` *<0-7>* This option sets the facility level of the first or second syslog host displayed. The default is 0. **Command mode:** Global configuration
`logging source-interface loopback` *<1-5>* Sets the loopback interface number for syslogs. **Command mode:** Global configuration
`logging console` Enables delivering syslog messages to the console. It is enabled by default. **Command mode:** Global configuration
`no logging console` Disables delivering syslog messages to the console. When necessary, disabling `console` ensures the switch is not affected by syslog messages. It is enabled by default. **Command mode:** Global configuration
[no] `logging synchronous` [`level` *<0-7>*	`all`] Enables or disables synchronous logging messages. When enabled, logging messages are displayed asynchronously. 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. `All` displays all messages asynchronously, regardless the severity level. The default setting is 2. **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

Table 129. Host Log Configuration Options (continued)

Command Syntax and Usage
`no logging console severity` Disables delivering syslog messages to the console based on severity. **Command mode:** Global configuration
[no] `logging log` [<*feature*>] Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as `vlans`, `stg`, or `ssh`), or enable/disable syslog on all available features. **Command mode:** Global configuration
`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
`show logging` [severity <*severity level*>] [reverse] Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 25. **Command mode:** All

SSH Server Configuration

For the RackSwitch G8124, these commands enable Secure Shell access from any SSH client.

Table 130. SSH Server Configuration Options

Command Syntax and Usage
ssh scp-password Set the administration password for SCP access. **Command mode:** Global configuration
ssh generate-host-key Generate the RSA host key. **Command mode:** Global configuration
ssh port *<TCP port number>* Sets the SSH server port number. **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
ssh maxauthattempts *<1-20>* Sets the maximum number of SSH authentication attempts. The default value is 2. **Command mode:** Global configuration
no ssh maxauthattempts Reset to its default value the maximum number of SSH authentication attempts. **Command mode:** Global configuration
ssh scp-enable Enables the SCP apply and save. **Command mode:** Global configuration
no ssh scp-enable Disables the SCP apply and save. **Command mode:** Global configuration
ssh enable Enables the SSH server. **Command mode:** Global configuration
no ssh enable Disables the SSH server. **Command mode:** Global configuration

Table 130. SSH Server Configuration Options (continued)

Command Syntax and Usage

`show ssh`
 	
    Displays the current SSH server configuration.
 	
    Command mode: All

`show ssh-clientpubkey {all|index <1-100>|username <user name>}`
 	
    Displays the current SSH public key configuration.
 	
    Command mode: All

`clear ssh-clientpubkey {all|index <1-100>|username <user name>}`
 	
    Clears stored public key configuration.
 	
    Command mode: All

RADIUS Server Configuration

Table 131. RADIUS Server Configuration Options

Command Syntax and Usage

`[no] radius-server primary-host <IP address>`
 	
    Sets the primary RADIUS server address.
 	
    Command mode: Global configuration

`[no] radius-server secondary-host <IP address>`
 	
    Sets the secondary RADIUS server address.
 	
    Command mode: Global configuration

`radius-server primary-host <IP address> key <1-32 characters>`
 	
    This is the primary shared secret between the switch and the RADIUS server(s).
 	
    Command mode: Global configuration

`radius-server secondary-host <IP address> key <1-32 characters>`
 	
    This is the secondary shared secret between the switch and the RADIUS server(s).
 	
    Command mode: Global configuration

`[default] radius-server port <UDP port number>`
 	
    Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.
 	
    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 131. RADIUS Server Configuration Options (continued)

Command Syntax and Usage
`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] 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 secure-backdoor` Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (`telnet`) is enabled. **Command mode:** Global configuration
`radius-server enable` Enables the RADIUS server. **Command mode:** Global configuration
`no radius-server enable` Disables the RADIUS server. **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 132. TACACS+ Server Configuration Options

Command Syntax and Usage
[no] tacacs-server primary-host *<IP address>* Defines the primary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server secondary-host *<IP address>* Defines the secondary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server primary-host *<IP address>* key *<1-32 characters>* This is the primary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] tacacs-server secondary-host *<IP address>* key *<1-32 characters>* This is the secondary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] tacacs-server primary-host [data-port|mgta-port|mgtb-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 secondary-host [data-port|mgta-port|mgtb-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

Table 132. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
[no] `tacacs-server chpassp` *<1-32 characters>* Defines the password for the primary TACACS+ server. **Command mode:** Global configuration
[no] `tacacs-server chpasss` *<1-32 characters>* Defines the password for the secondary TACACS+ server. **Command mode:** Global configuration
[default] `tacacs-server port` *<TCP port number>* Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49. **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
`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
`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
`ip tacacs-server source-interface loopback` *<1-5>* Sets the TACACS+ source loopback interface. **Command mode:** Global configuration
[no] `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

Table 132. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
[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 G8124, contact your Service and Support line. **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
[no] tacacs-server privilege-mapping Enables or disables TACACS+ privilege-level mapping. The default value is disabled. **Command mode:** Global configuration
[no] tacacs-server password-change Enables or disables TACACS+ password change. The default value is disabled. **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

Table 132. TACACS+ Server Configuration Options (continued)

Command Syntax and Usage
[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
[no] tacacs-server directed-request Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, 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: – Restricted: Only the username is sent to the specified TACACS+ server. – No-truncate: The entire login string is sent to the TACACS+ server. **Command mode:** Global configuration
[no] tacacs-server accounting-enable Enables or disables TACACS+ accounting. **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
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 133. LDAP Server Configuration Options

Command Syntax and Usage
[no] ldap-server primary-host *<IP address>* [data-port|mgta-port| mgtb-port]   Sets the primary LDAP server address.   **Command mode:** Global configuration
[no] ldap-server secondary-host *<IP address>* [data-port|mgta-port| mgtb-port]   Sets the secondary LDAP server address.   **Command mode:** Global configuration
[default] ldap-server port *<UDP port number>*   Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389.   **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 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
ldap-server domain [*<1-128 characters>*|none]   Sets the domain name for the LDAP server. Enter the full path for your organization. For example: ou=people,dc=mydomain,dc=com   **Command mode:** Global configuration
[no] ldap-server backdoor   Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.   To obtain the LDAP back door password for your G8124, contact your Service and Support line.   **Command mode:** Global configuration

Table 133. LDAP Server Configuration Options (continued)

Command Syntax and Usage
`ldap-server attribute username` *<1-128 characters>* Sets a customized LDAP user attribute. The defaul value is `uid`. The user attribute needs to be set to `cn` if LDAP server is MS active directory. **Command mode:** Global configuration
`no ldap-server attribute` Sets the LDAP user attribute back to its default value. **Command mode:** Global configuration
`ldap-server enable` Enables the LDAP server. **Command mode:** Global configuration
`no ldap-server enable` Disables the LDAP server. **Command mode:** Global configuration
`show ldap-server` Displays the current LDAP server parameters. **Command mode:** All

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 134. NTP Server Configuration Options

Command Syntax and Usage
[no] ntp primary-server {*<host name>*|*<IP address>*}   Prompts for the hostname or IP addresses of the primary NTP server to which you want to synchronize the switch clock.   **Command mode:** Global configuration
[no] ntp ipv6 primary-server *<IPv6 address>*   Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock.   **Note**: To delete the IPv6 primary server, use the following command: no ntp primary-server *<IP address>*   **Command mode:** Global configuration
[no] ntp ipv6 secondary-server *<IPv6 address>*   Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock.   **Note**: To delete the IPv6 secondary server, use the following command: no ntp secondary-server *<IP address>*   **Command mode:** Global configuration
[no] ntp secondary-server {*<host name>*|*<IP address>*}   Prompts for the hostname or IP addresses of the secondary NTP server to which you want to synchronize the switch clock.   **Command mode:** Global configuration
[no] ntp sync-logs   Enables or disables informational logs for NTP synchronization failures. Default setting is enabled.   **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.   **Command mode:** Global configuration
no ntp offset   Resets the NTP offset to the default 300 seconds value.   **Command mode:** Global configuration

Table 134. NTP Server Configuration Options (continued)

Command Syntax and Usage
`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 source loopback` *<1-5>* Sets the NTP source loopback interface. **Command mode:** Global configuration
`ntp enable` Enables the NTP synchronization service. **Command mode:** Global configuration
`no ntp enable` Disables the NTP synchronization service. **Command mode:** Global configuration
`show ntp` Displays the current NTP service settings. **Command mode:** All

System SNMP Configuration

IBM N/OS 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 135. System SNMP Options

Command Syntax and Usage
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
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
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
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

Table 135. System SNMP Options (continued)

Command Syntax and Usage
[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
snmp-server write-community *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is *private*. **Command mode:** Global configuration
snmp-server trap-source {*<interface number>*|loopback *<1-5>*} Configures the source interface for SNMP traps. To send traps through the management port A, specify interface 127. To send traps through management port B, specify interface 128. **Command mode:** Global configuration
snmp-server host *<trap host IP address>* *<trap host community string>* Adds a trap host server. **Command mode:** Global configuration
no snmp-server host *<trap host IP address>* Removes the trap host server. **Command mode:** Global configuration
snmp-server timeout *<1-30>* Sets the timeout value for the SNMP state machine, in minutes. **Command mode:** Global configuration
[no] snmp-server authentication-trap Enables or disables the use of the system authentication trap facility. The default setting is disabled. **Command mode:** Global configuration
[no] snmp-server link-trap Enables or disables globally the sending of SNMP link up and link down traps. The default setting is enabled. **Command mode:** Global configuration
[no] snmp-server link-trap port *<port alias or number>* 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
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 136. SNMPv3 Configuration Options

Command Syntax and Usage
`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.   **Command mode:** Global configuration   To view command options, see page 227.
`snmp-server view <1-128>`   This command allows you to create different MIB views.   **Command mode:** Global configuration   To view command options, see page 228.
`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.   **Command mode:** Global configuration   To view command options, see page 229.
`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.   **Command mode:** Global configuration   To view command options, see page 230.
`snmp-server community <1-16>`   The community table contains objects for mapping community strings and version-independent SNMP message parameters.   **Command mode:** Global configuration   To view command options, see page 231.

Table 136. SNMPv3 Configuration Options (continued)

`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. **Command mode:** Global configuration To view command options, see .
`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. **Command mode:** Global configuration To view command options, see .
`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. **Command mode:** Global configuration To view command options, see .
`snmp-server version {v1v2v3│v3only}` This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. This command is enabled by default. **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 137. User Security Model Configuration Options

Command Syntax and Usage
snmp-server user *<1-16>* 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 *<1-16>* authentication-protocol {md5|sha|none} authentication-password *<password value>* 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 *<1-16>* privacy-protocol {des|aes|none} privacy-password *<password value>* 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 des (CBC-DES Symmetric Encryption Protocol), aes (AES-128 Advanced Encryption Standard Protocol) or 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 137. User Security Model Configuration Options

Command Syntax and Usage
`no snmp-server user` *<1-16>* 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 138. SNMPv3 View Configuration Options

Command Syntax and Usage
`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` *<1-64 characters>* This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. **Command mode:** Global configuration
`[no] 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>* `type {included|excluded}` This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is 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 139. View-based Access Control Model Options

Command Syntax and Usage
snmp-server access *<1-32>* name *<1-32 characters>*   Defines the name of the group.   **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>* level {noAuthNoPriv|authNoPriv|authPriv}   Defines the minimum level of security required to gain access rights. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The 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>* 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>* 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
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
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

Table 140. SNMPv3 Group Configuration Options

Command Syntax and Usage
`snmp-server group` *<1-16>* `security {usm`|`snmpv1`|`snmpv2}` Defines the security model. **Command mode:** Global configuration
`snmp-server group` *<1-16>* `user-name` *<1-32 characters>* Sets the user name as defined in the following command on page 227: `snmp-server user` *<1-16>* `name` *<1-32 characters>* **Command mode:** Global configuration
`snmp-server group` *<1-16>* `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 227. **Command mode:** Global configuration
`no snmp-server group` *<1-16>* 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 141. 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 on :
 `snmp-server user <1-16> name <1-32 characters>`
 	
 Command string: 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
`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
`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 142. 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>* `name` *<1-32 characters>* `address` *<transport IP address>* Configures a transport IPv4 or 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>* `port` *<port range>* 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
`snmp-server target-address` *<1-16>* `parameters-name` *<1-32 characters>* Defines the name as defined in the following command on : `snmp-server target-parameters` *<1-16>* `name` *<1-32 characters>* **Command mode:** Global configuration
`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 143. Target Parameters Table Configuration Options

Command Syntax and Usage
`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

`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>* `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 227) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration

`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. The level noAuthNoPriv means that the SNMP message will be sent without authentication and without using a privacy protocol. The level authNoPriv means that the SNMP message will be sent with authentication but without using a privacy protocol. The authPriv means that the SNMP message will be sent both with authentication and using a privacy protocol.
 	
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 144. 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

Table 145. System Access Configuration Options

Command Syntax and Usage
`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 128 characters) and confirmation of the new password. **Note:** To disable the user account, set the password to null (no password). **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 128 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 administrator-password` Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the G8124, 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 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Note:** You cannot disable the administrator password. **Command Mode**: Global configuration
`[no] access user password-recovery` Enables or disables the password fix-up mode. The user can change the password of the administrator. By default, this feature is `enabled`. **Command Mode**: Global configuration
`access user password-recovery`
`[no] access http enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default. **Command mode:** Global configuration

Table 145. System Access Configuration Options (continued)

Command Syntax and Usage
[default] access http port [<*port alias or number*>] Sets the switch port used for serving switch Web content. The default is HTTP port 80. **Command mode:** Global configuration
[no] access snmp {read-only|read-write} Disables or provides read-only/write-read SNMP access. **Command mode:** Global configuration
[no] access telnet enable Enables or disables Telnet access. This command is enabled by default. **Command mode:** Global configuration
[default] access telnet port [<*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 tftp-port [<*1-65535*>] Sets the TFTP port for the switch. The default is port 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 146. Management Network Configuration Options

Command Syntax and Usage
`access management-network` *<mgmt network IPv4 or IPv6 address>* *<mgmt network mask or prefix length>* Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the IBM N/OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP 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 or IPv6 address>* *<mgmt network mask or prefix length>* Removes a defined network, which consists of a management network address and a management network mask address. **Command mode:** Global configuration
`access management-network` *<mgmt network IPv4 address>* *<mgmt network mask>* {`snmp-ro`|`snmp-rw`} Adds a defined IPv4 network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IP address and mask address in dotted-decimal notation. **Command mode:** Global configuration
`access management-network6` *<mgmt network IPv6 address>* *<IPv6 prefix length>* {`snmp-ro`|`snmp-rw`} Adds a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed. **Command mode:** Global configuration
`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` {`snmp-ro`|`snmp-rw`} Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration

Table 146. Management Network Configuration Options

Command Syntax and Usage
`show access management-network` Displays the current management network configuration. **Command mode:** All except User EXEC
`clear access management-network` Removes all defined management networks. **Command mode:** Global configuration

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 147. 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
`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 148. 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>* Configures the TCP port used for NETCONF. The default port number is 830. **Command mode:** Global configuration

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 149. User Access Control Configuration Options

Command Syntax and Usage
`access user` *<1-20>`* Configures the User ID. **Command mode:** Global configuration
`access user eject {`*<user name>*`/`*<session ID>*`}` Ejects the specified user from the G8124. **Command mode:** Global configuration
`clear line` *<1-12>* Ejects the user with the corresponding session ID from the G8124. **Command mode:** Privileged EXEC
`[no] access user administrator-enable` Enables or disables the default administrator account. **Command mode:** Global configuration
`access user user-password` Sets the user (`user`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user operator-password` Sets the operator (`oper`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user administrator-password` Sets the administrator (`admin`) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Command mode:** Global configuration
`show access user` Displays the current user status. **Command mode:** All except User EXEC

System User ID Configuration

Table 150. User ID Configuration Options

Command Syntax and Usage
`access user `*`<1-20>`*` level {user|operator|administrator}` Sets the Class-of-Service to define the user's authority level. IBM N/OS 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 128 characters) and confirmation of the new password. **Command mode:** Global configuration
`access user `*`<1-20>`*` enable` Enables the user ID. **Command mode:** Global configuration
`no access user `*`<1-20>`*` enable` Disables the user ID. **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:** All except User EXEC

Strong Password Configuration

Table 151. Strong Password Configuration Options

Command Syntax and Usage
`access user strong-password enable` Enables Strong Password requirement. **Command mode:** Global configuration
`no access user strong-password enable` 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 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
`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
`show access user strong-password` Displays the current Strong Password configuration. **Command mode:** All except User EXEC

HTTPS Access Configuration

Table 152. 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
`[default] access https port [<`*TCP port number*`>]` Defines the HTTPS Web server port number. The default port is 443. **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: – Country Name (2 letter code): CA – State or Province Name (full name): Ontario – Locality Name (for example, city): Ottawa – Organization Name (for example, company): Blade – Organizational Unit Name (for example, section): Operations – Common Name (for example, user's name): Mr Smith – Email (for example, email address): info@bladenetwork.net 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
`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
`copy {tftp|sftp} ca-cert address <`*hostname or server-IP-addr*`> filename <`*server-filename*`>` Enables you to import a certificate authority root certificate using TFTP/SFTP. **Command mode:** Global configuration
`copy {tftp|sftp} host-key address <`*hostname or server-IP-addr*`> filename <`*server-filename*`>` Enables you to import a host private key using TFTP/SFTP. **Command mode:** Global configuration

Table 152. HTTPS Access Configuration Options (continued)

Command Syntax and Usage
`copy {tftp|sftp} host-cert address` *<hostname or server-IP-addr>* `filename` *<server-filename>* Enables you to import a host certificate using TFTP/SFTP. **Command mode:** Global configuration
`show access` Displays the current SSL Web Access configuration. **Command mode:** All except User 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 153. Custom DST Options

Command Syntax and Usage

`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

`system custom-dst enable`   Enables the Custom Daylight Saving Time settings.   **Command mode:** Global configuration
`no system custom-dst enable`   Disables the Custom Daylight Saving Time settings.   **Command mode:** Global configuration
`show custom-dst`   Displays the current Custom DST configuration.   **Command mode:** All except User EXEC

sFlow Configuration

IBM N/OS 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 154. sFlow Configuration Options

Command Syntax and Usage
`sflow enable` Enables the sFlow agent. **Command mode:** Global configuration
`no sflow enable` Disables the sFlow agent. **Command mode:** Global configuration
`sflow server` *<IP address>* `[data-port|mgta-port|mgtb-port]` Defines the sFlow server address and interface port. **Command mode:** Global configuration
`sflow port` *<1-65535>* Configures the UDP port for the sFlow server. The default value is `6343`. **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 155. sFlow Port Configuration Options

Command Syntax and Usage
`[no] sflow polling` *<5-60>* Configures the sFlow polling interval, in seconds. The default setting is `disabled`. **Command mode:** Interface port
`[no] sflow sampling` *<1-16777215>* Configures the sFlow sampling rate, in packets per sample. The default setting is `disabled`. **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 156. Server Port Configuration Options

Command Syntax and Usage
`system server-ports port` *<port alias or number>* Adds one or more port physical ports to the list of server ports. **Command mode:** Global configuration
`no system server-ports port` *<port alias or number>*   Removes one of more ports from 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 157. Port Configuration Options

Command Syntax and Usage
interface port *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
interface portchannel *<trunk number>*|lacp *<1-65535>* Enter Interface portchannel mode. These commands allow you to configure port parameters for all port members in the selected trunk group (portchannel). **Command mode:** Global configuration
dot1p *<0-7>* Configures the port's 802.1p priority level. **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] bpdu-guard Enables or disables BPDU guard, to avoid Spanning-Tree loops on ports configured as edge ports. **Command mode:** Interface port/Interface portchannel
[no] dscp-marking Enables or disables DSCP re-marking on a port. **Command mode:** Interface port/Interface portchannel
[no] switchport Enables or disables routing on a port. **Command mode:** Interface port

Table 157. Port Configuration Options (continued)

Command Syntax and Usage

`switchport mode {access|trunk|private-vlan}`
 	
    Configures the port's trunking mode:
 	
    – `access` allows association to a single VLAN
 	
    – `trunk` allows association to multiple VLANs.
 	
    – `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

`switchport mode private-vlan {host|promiscuous|trunk promiscuous| trunk secondary}`
 	
    Configures port behavior when associated to a private VLAN. Private VLANs allow definition of VLAN sub-domains within a primary VLAN domain, usually for the purpose of enabling Layer 2 partitioning over a single Layer 3 subnet.
 	
    – `host` ports are associated to a secondary VLAN within the private VLAN
 	
    – `promiscuous` ports are associated to the primary VLAN within the private VLAN.
 	
    – `trunk promiscuous` ports behave like promiscuous ports within the private VLAN domain, but can also belong to regular VLANs.
 	
    – `trunk secondary` ports behave like secondary isolated ports within the private VLAN domain, but can also belong to regular VLANs.
 	
    Command mode: Interface port/Interface portchannel

`switchport access vlan <`*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

`switchport trunk native vlan <`*1-4094*
 	
    Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. Default value is 1 for data ports and 4095 for the management port.
 	
    Command mode: Interface port/Interface portchannel

Table 157. Port Configuration Options (continued)

Command Syntax and Usage
`switchport trunk allowed vlan [add|remove] `*`<VLAN ID range>`* Updates the associated VLANs in trunk mode. – `add` enables the VLAN range in addition to the current configuration – `remove` eliminates the VLAN range from the current configuration **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {all|none}` – `all` associates all existing and enabled VLANs to the port. This is an operational command applicable only to VLANs currently configured at the moment of execution. VLANs created afterward will not be associated automatically. Also, as an operational command, it will not be dumped into the configuration file. – `none` removes the port from all currently associated VLANS except the default VLAN **Command mode:** Interface port/Interface portchannel
[no] `switchport private-vlan mapping `*`<primary VLAN>`* Enables or disables private VLAN mapping on a port in promiscuous mode. **Command mode:** Interface port/Interface portchannel
[no] `switchport private-vlan association `*`<primary VLAN> <secondary VLAN>`* Enables or disables the private VLAN association on a secondary port. **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
[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
[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

Table 157. Port Configuration Options (continued)

Command Syntax and Usage
[no] learning Enables or disables FDB learning on the port. **Command mode:** Interface port/Interface portchannel
port-channel min-links *<1-12>* Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the down state. **Command mode:** Interface port
storm-control {broadcast|multicast|unicast} level pps *<100-10000>* Limits the number of broadcast, multicast or unicast packets per second 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] ip dhcp snooping trust Configures this port as a trusted port for DHCP packets from the server. **Command mode:** Interface port
ip dhcp snooping limit rate *<1-2048>* Configures the maximum number of DHCP packets allowed per second. **Command mode:** Interface port
no shutdown Enables the 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 253.) **Command mode:** Interface port/Interface portchannel
show interface port *<port alias or number>* Displays current port 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 158. Port Error Disable Options

Command Syntax and Usage
`errdisable recovery` Enables 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
`no errdisable recovery` Enables automatic error-recovery for the port. **Command mode:** Interface port/Interface portchannel
`show interface port` *<port alias or number>* `errdisable` Displays current port Error Disable parameters. **Command mode:** All

Port Link Flap Dampening Configuration

Table 159. Port Link Flap Dampening Configuration Options

Command Syntax and Usage
`errdisable link-flap enable` Enables Link Flap Dampening on the port. For more information, see "Link Flap Dampening Configuration" on page 209. **Command mode:** Interface port
`no errdisable link-flap enable` Disables Link Flap Dampening on the port. **Command mode:** Interface port
`show interface port` *<port alias or number>* `errdisable link-flap` Displays the current Link Flap Dampening parameters for the port. **Command mode:** All

Port Link Configuration

Use these commands to set flow control for the port link.

Table 160. Port Link Configuration Options

Command Syntax and Usage
`speed {10000}` Sets the link speed. Some options are not valid on all ports. The choices include: – 10000 Mps – any (auto negotiate port speed) **Command mode:** Interface port/Interface portchannel
`duplex {full|half|auto}` 　　Sets the operating mode. The choices include: 　　– "Auto negotiation (default) 　　– Half-duplex 　　– Full-duplex 　　**Note**: Data ports are fixed at full duplex. 　　**Command mode:** Interface port/Interface portchannel
`flowcontrol receive {on|off}` 　　Enables or disables flow control receive. 　　**Command mode:** Interface port/Interface portchannel
`flowcontrol send {on|off}` 　　Enables or disables flow control transmit. 　　**Command mode:** Interface port/Interface portchannel
`[no] auto` 　　Turns auto-negotiation on or off. 　　**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
`show interface port` *<port alias or number>* 　　Displays current port 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:

```
G8124(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 G8124 is reset. See the "Operations Commands" on page 433 for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 161. 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: – **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. – **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 number> udld` Displays current port 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 162. Port OAM Configuration Options

Command Syntax and Usage
`oam [passive]`   Configures the OAM discovery mode, as follows: – `Passive`: This 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/
`no oam [passive]`   Disables OAM discovery on the port.   **Command mode:** Interface port
`show interface port <port number> oam`   Displays current port OAM parameters.   **Command mode:** All

Port ACL Configuration

Table 163. ACL/QoS Configuration Options

Command Syntax and Usage
`access-control list` *\<ACL number\>* Adds 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 list` *\<ACL number\>* Removes the specified ACL list from the port. **Command mode:** Interface port/Interface portchannel
`access-control list6` *\<ACL number\>* Adds 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/Interface portchannel
`no access-control list6` *\<ACL number\>* Removes the specified IPv6 ACL list from the port. **Command mode:** Interface port/Interface portchannel
`access-control group` *\<ACL group number\>* Adds 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 group` *\<ACL group number\>* Removes the specified ACL group from the port. **Command mode:** Interface port/Interface portchannel
`show interface port` *\<port alias or number\>* `access-control` Displays current ACL QoS parameters. **Command mode:** All

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 G8124 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 164. 802.1p Configuration Options

Command Syntax and Usage
qos transmit-queue mapping *<priority (0-7)>* *<COSq number>*   Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue that handles the matching traffic.   **Command mode:** Global configuration
qos transmit-queue weight-cos *<COSq number>* *<weight (0-15)>*   Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).   **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 165. DSCP Configuration Options

Command Syntax and Usage
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 (0-63) of incoming packets, followed by the new value. **Command mode:** Global configuration
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 re-marking Turns on DSCP re-marking globally. **Command mode:** Global configuration
no qos dscp re-marking Turns off DSCP re-marking globally. **Command mode:** Global configuration
show qos dscp Displays the current DSCP parameters. **Command mode:** All

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 .

Table 166. General ACL Configuration Options

Command Syntax and Usage
[no] `access-control list` <*1-127*> Configures an Access Control List. To view command options, see page 259. **Command mode:** Global configuration
[no] `access-control list6` <*1-128*> Configures an Access Control List. To view command options, see page 266. **Command mode:** Global configuration
[no] `access-control macl` <*1-127*> Configures an Access Control List. To view command options, see page 259. **Command mode:** Global configuration
[no] `access-control vmap` <*1-127*> Configures an ACL VLAN map. To view command options, see page 271. **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 167. ACL Configuration Options

Command Syntax and Usage
`access-control list <1-127> action {permit｜deny｜set-priority <0-7>｜change-vlan <1-4094>}` 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 (0-7) or change the 802.1Q VLAN ID. **Command mode:** Global configuration
`[no] access-control list <1-127> statistics` Enables or disables the statistics collection for the Access Control List. **Command mode:** All except User EXEC
`[no] access-control list <1-127> 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
`default access-control list <1-127>` Resets the ACL parameters to their default values. **Command mode:** Global configuration
`show access-control list <1-127>` 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 168. ACL Port Mirroring Options

Command Syntax and Usage
`access-control list <1-127> mirror port <port alias or number>｜none` Configures the destination to which packets that match this ACL are mirrored. **Command mode:** Global configuration

Table 168. ACL Port Mirroring Options

Command Syntax and Usage
`no access-control list <1-127> mirror`   Removes all mirrored packets.   **Command mode:** Global configuration
`show access-control list <1-127> 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 169. Ethernet Filtering Configuration Options

Command Syntax and Usage

`access-control list <1-127> ethernet`
 `source-mac-address <MAC address> <MAC mask>`
 Defines the source MAC address for this ACL.
 Command mode: Global configuration

`no access-control list <1-127> ethernet source-mac-address`   Removes the source MAC address for this ACL.   **Command mode:** Global configuration

`access-control list <1-127> ethernet`
 `destination-mac-address <MAC address> <MAC mask>`
 Defines the destination MAC address for this ACL.
 Command mode: Global configuration

`no access-control list <1-127> ethernet destination-mac-address`   Removes the destination MAC address for this ACL.   **Command mode:** Global configuration
`access-control list <1-127> ethernet vlan <VLAN ID> <VLAN mask>`   Defines a VLAN number and mask for this ACL.   **Command mode:** Global configuration
`no access-control list <1-127> ethernet vlan`   Removes VLAN number and mask for this ACL.   **Command mode:** Global configuration

`access-control list <1-127> ethernet ethernet-type`
 `{arp|ip|ipv6|mpls|rarp|any|<other (0x600-0xFFFF)>}`
 Defines the Ethernet type for this ACL.
 Command mode: Global configuration

Table 169. Ethernet Filtering Configuration Options

Command Syntax and Usage

`no access-control list <1-127> ethernet ethernet-type`
 	
    Removes the Ethernet type for this ACL.
 	
    Command mode: Global configuration

`access-control list <1-127> ethernet priority <0-7>`
 	
    Defines the Ethernet priority value for the ACL.
 	
    Command mode: Global configuration

`no access-control list <1-127> ethernet priority`
 	
    Removes the Ethernet priority value for the ACL.
 	
    Command mode: Global configuration

`default access-control list <1-127> ethernet`
 	
    Resets Ethernet parameters for the ACL to their default values.
 	
    Command mode: Global configuration

`no access-control list <1-127> ethernet`
 	
    Removes Ethernet parameters for the ACL.
 	
    Command mode: Global configuration

`show access-control list <1-127> 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 170. IP version 4 Filtering Configuration Options

Command Syntax and Usage

`[no] access-control list <1-127> 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 <1-127> 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

Table 170. IP version 4 Filtering Configuration Options

Command Syntax and Usage
[no] `access-control list` *<1-127>* `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` *<1-127>* `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
`default access-control list` *<1-127>* `ipv4` Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
`show access-control list` *<1-127>* `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 171. TCP/UDP Filtering Configuration Options

Command Syntax and Usage
[no] access-control list *<1-127>* 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 *<1-127>* 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 *<1-127>* tcp-udp flags *<value (0x0-0x3f)>* *<mask (0x0-0x3f)>*
Defines a TCP/UDP flag for the ACL.
Command mode: Global configuration
default access-control list *<1-127>* tcp-udp
Resets the TCP/UDP parameters for the ACL to their default values.
Command mode: Global configuration
show access-control list *<1-127>* tcp-udp
Displays the current TCP/UDP Filtering parameters.
Command mode: All

ACL Metering Configuration

These commands define the Access Control profile for the selected ACL.

Table 172. ACL Metering Configuration Options

Command Syntax and Usage
`access-control list <1-127> meter committed-rate <64-10000>` Configures the committed rate, in megabits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
`access-control list <1-127> 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
`[no] access-control list <1-127> meter enable` Enables or disables ACL Metering. **Command mode:** Global configuration
`access-control list <1-127> meter action {drop|pass}` Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
`default access-control list <1-127> meter` Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
`no access-control list <1-127> meter` Deletes the selected ACL meter. **Command mode:** Global configuration
`show access-control list <1-127> 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.

Re-Marking In-Profile Configuration

Table 173. ACL Re-Marking In-Profile Options

Command Syntax and Usage
`[no] access-control list <1-127> re-mark in-profile 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] no access-control list <1-127> re-mark in-profile dscp <0-63>` Remarks the DSCP value for in-profile traffic. **Command mode:** Global configuration
`[no] no access-control list <1-127> 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
`default access-control list <1-127> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list <1-127> re-markS` Displays current re-mark parameters. **Command mode:** All

Re-Marking Out-of-Profile Configuration

Table 174. ACL Re-Marking Out-of-Profile Options

Command Syntax and Usage
`access-control list <1-127> re-mark out-profile dscp <1-63>` Re-marks the DSCP value on out-of-profile packets for the ACL. **Command mode:** Global configuration
`no access-control list <1-127> re-mark out-profile` Disables re-marking on out-of-profile traffic. **Command mode:** Global configuration
`show access-control list <1-127> re-mark` Displays current re-mark parameters. **Command mode:** All

ACL IPv6 Configuration

These commands allow you to define filtering criteria for each IPv6 Access Control List (ACL).

Table 175. 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 (0-7). **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
`[no] access-control list6 <1-128> log` Enables or disables Access Control List logging.
`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

IP version 6 Filtering Configuration

These commands allow you to define IPv6 matching criteria for an ACL.

Table 176. IP version 6 Filtering Options

Command Syntax and Usage
[no] `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 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 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 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 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
`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 177. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
[no] access-control list6 *<1-128>* 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 list6 *<1-128>* 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 sport above. **Command mode:** Global configuration
[no] 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
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.

IPv6 Re-Marking In-Profile Configuration

Table 178. IPv6 Re-Marking In-Profile Options

Command Syntax and Usage
[no] 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-control list6 *<1-128>* re-mark in-profile dscp *<0-63>*   Re-marks the DSCP value for in-profile traffic.   **Command mode:** Global configuration
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 Metering Configuration

These commands define the Access Control profile for the selected ACL.

IPv6 Metering Configuration

Table 179. IPv6 Metering Options

Command Syntax and Usage
access-control list6 *<1-127>* meter committed-rate *<64-10000>*   Configures the committed rate, in megabits per second. The committed rate must be a multiple of 64.   **Command mode:** Global configuration
access-control list6 *<1-127>* 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
[no] access-control list6 *<1-127>* meter enable   Enables or disables ACL Metering.   **Command mode:** Global configuration

Table 179. IPv6 Metering Options

Command Syntax and Usage
`access-control list6 <1-127> meter action {drop|pass}` Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
`default access-control list6 <1-127> meter` Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
`no access-control list6 <1-127> meter` Deletes the selected ACL meter. **Command mode:** Global configuration
`show access-control list6 <1-127> 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 180. ACL Log Configuration Options

Command Syntax and Usage
`access-control list <1-127> log` Enables access control list logging. **Command mode:** Global configuration
`access-control log interval <seconds>` Sets the filter log displaying interval in seconds. **Command mode:** Global configuration
`access-control log rate-limit <seconds>` Sets the filter log queue rate limit in seconds. **Command mode:** Global configuration
`default access-control log [interval	rate-lmt]` 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

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 259.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration" on page 306.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 420.

Table 181. lists the general VMAP configuration commands.

Table 181. VMAP Configuration Options

Command Syntax and Usage
`access-control vmap `*`<1-127>`*` 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 (0-7). **Command mode:** Global configuration
`[no] access-control vmap `*`<1-127>`*` ipv4 source-ip-address` *`<IPv4 address>`* *`<IPv4 mask>`* Enables or disables filtering of VMAP statistics collection based on source IP address. **Command mode:** Global configuration
`[no] access-control vmap `*`<1-127>`*` ipv4 destination-ip-address` *`<IPv4 address>`* *`<IPv4 mask>`* Enables or disables filtering of VMAP statistics collection based on destination IP address. **Command mode:** Global configuration
`[no] access-control vmap `*`<1-127>`*` ipv4 protocol `*`<0-255>`* Enables or disables filtering of VMAP statistics collection based on protocol. **Command mode:** Global configuration
`[no] access-control vmap `*`<1-127>`*` ipv4 type-of-service `*`<0-255>`* Enables or disables filtering of VMAP statistics collection based on type of service. **Command mode:** Global configuration
`access-control vmap `*`<1-127>`*` meter enable` Enables ACL port metering. **Command mode:** All except User EXEC

Table 181. VMAP Configuration Options

Command Syntax and Usage
`access-control vmap <1-127> meter action drop|pass` Sets ACL port metering to drop or pass out-of-profile traffic. **Command mode:** Global configuration
`access-control vmap <1-127> meter committed-rate <64-10000000>` Sets the ACL port metering control rate in kilobits per second. **Command mode:** Global configuration
`access-control vmap <1-127> meter maximum-burst-size <32-4096>` Sets the ACL port metering maximum burst size in kilobytes. The following eight values are allowed: – 32 – 64 – 128 – 256 – 512 – 1024 – 2048 – 4096 **Command mode:** Global configuration
`no access-control vmap <1-127> meter enable` Disables ACL port metering. **Command mode:** Global configuration
`access-control vmap <1-127> mirror port <port>` Sets the specified port as the mirror target. **Command mode:** Global configuration
`no access-control vmap <1-127> mirror` Turns off ACL mirroring. **Command mode:** Global configuration
`access-control vmap <1-127> packet-format ethernet ethernet-type2|llc|snap` Sets to filter the specified ethernet packet format type. **Command mode:** Global configuration
`access-control vmap <1-127> packet-format ip ipv4|ipv6` Sets to filter the specified IP packet format type. **Command mode:** Global configuration

Table 181. VMAP Configuration Options

Command Syntax and Usage
`access-control vmap <1-127> packet-format tagging any|none|tagged` Sets to filter the based on packet tagging. The options are: – `any`: Filter tagged & untagged packets – `none`: Filter only untagged packets – `tagged`: Filter only tagged packets **Command mode:** Global configuration
`no access-control vmap <1-127> packet-format ethernet|ip|tagging` Disables filtering based on the specified packet format. **Command mode:** Global configuration
`access-control vmap <1-127> re-mark dot1p <0-7>` Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
`no access-control vmap <1-127> re-mark dot1p <0-7>` Disables the use of dot1p for in-profile traffic ACL re-mark configuration. **Command mode:** Global configuration
`access-control vmap <1-127> re-mark in-profile|out-profile dscp <0-63>` Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
`no access-control vmap <1-127> re-mark in-profile|out-profile` Removes all re-mark in-profile or out-profile settings. **Command mode:** Global configuration
`[no] access-control vmap <1-127> re-mark use-tos-precedence` Enables or disables the use of the TOS precedence for in-profile traffic. **Command mode:** Global configuration
`[no] access-control vmap <1-127> statistics` Enables or disables statistics for this access control list. **Command mode:** Global configuration
`access-control vmap <1-127> 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 <1-127> tcp-udp [<flags mask (0x0-0x3F)>]` Sets the TCP flags for this ACL. **Command mode:** Global configuration

Table 181. VMAP Configuration Options

Command Syntax and Usage
`no access-control vmap` *<1-127>* `tcp-udp` Removes TCP/UDP filtering for this ACL. **Command mode:** Global configuration
`default access-control vmap` *<1-127>* Resets the VMAP parameters to their default values. **Command mode:** Global configuration
`show access-control vmap` *<1-127>* Displays the current VMAP parameters. **Command mode:** All except User EXEC

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the G8124, see "Appendix A: Troubleshooting" in the *IBM N/OS 7.9 Application Guide*.

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 182. 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 except User EXEC

Port-Mirroring Configuration

Table 183. 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 mirrored port.
 	
    Command mode: Global configuration

`show port-mirroring`
 	
    Displays the current settings of the monitoring port.
 	
    Command mode: All except User EXEC

Layer 2 Configuration

The following table describes basic Layer 2 Configuration commands. The following sections provide more detailed information and commands.

Table 184. Layer 2 Configuration Commands

Command Syntax and Usage
`vlan` *<VLAN number>* Enter VLAN configuration mode. To view command options, see . **Command mode:** Global configuration
`show layer2` Displays current Layer 2 parameters. **Command mode:** All

Spanning Tree Configuration

IBM N/OS 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). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

Note: When VRRP is used for active/active redundancy, STG must be enabled.

Table 185. Spanning Tree Configuration Options

Command Syntax and Usage
`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 `spanning-tree mode disable`, the switch globally turns Spanning Tree `off`. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command. **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. **Note**: When using VASA, a maximum number of 128 automatically assigned STGs is supported. **Note**: VASA applies only to PVRST mode. **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 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. Configure 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

Table 185. Spanning Tree Configuration Options (continued)

Command Syntax and Usage
`[no] spanning-tree link-type {p2p|shared|auto}` Defines the type of link connected to the port, as follows: – `auto`: Configures the port to detect the link type, and automatically match its settings. – `p2p`: Configures the port for Point-To-Point protocol. – `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
`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
`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: – Priority – Hello interval – Maximum age value – Forwarding delay – Aging time You can also see the following port-specific STG information: – Port alias and priority – Cost – State **Command mode:** All

Table 185. Spanning Tree Configuration Options (continued)

Command Syntax and Usage
`show spanning-tree root` Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see . **Command mode:** All
`show spanning-tree blockedports` Lists the ports blocked by each STP instance. **Command mode:** All
`show spanning-tree [vlan <VLAN ID>] bridge` Displays Spanning Tree bridge information. For details, see . **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 186. Multiple Spanning Tree Configuration Options

Command Syntax and Usage
`spanning-tree mst configuration` Enables MSTP configuration mode. **Command mode:** Global configuration
`[no] 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] 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
`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. **Command mode:** Global configuration

Table 186. Multiple Spanning Tree Configuration Options (continued)

Command Syntax and Usage
[no] spanning-tree mst *\<instance number or range\>* enable Enables or disables the specified MSTP instance. **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. 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. Default value is 20. **Command mode:** Global configuration
default spanning-tree mst *\<instance number or range\>* Restores a Spanning Tree instance or range of instances to default configuration. **Command mode:** Global configuration
instance *\<0-32\>* vlan *\<VLAN numbers\>* 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 *\<1-32\>* vlan {*\<VLAN numbers\>*|all} Remove the specified VLANs or all VLANs from the Spanning Tree instance. **Command mode:** MST configuration
spanning-tree mst *\<instance number or range\>* priority *\<0-65535\>* Configures the CIST 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...); the default value is 32768. **Command mode:** Global configuration
no spanning-tree mst configuration Returns the MST region to its default values: no VLAN is mapped to any MST instance. Revision number is 1. **Command mode**: Global configuration

Table 186. Multiple Spanning Tree Configuration Options (continued)

Command Syntax and Usage
`show spanning-tree mst <instance number or range> information` Displays current MST information for the specified instance. **Command mode:** All
`show spanning-tree mst configuration` Displays the current MSTP settings. **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 187. MSTP Port Configuration Options

Command Syntax and Usage
`spanning-tree mst <instance number or range> 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
`spanning-tree mst <instance number or range> 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: – 1Gbps = 20000 – 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 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
`[no] spanning-tree pvst-protection` Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is `disabled`. **Command mode:** Interface port/Interface portchannel

Table 187. MSTP Port Configuration Options (continued)

Command Syntax and Usage
`[no] spanning-tree mst` *<instance number or range>* `enable` Enables or disables the specified MSTP instance on the port. **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

describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST) protocols.

Table 188. RSTP/PVRST Configuration Options

Command Syntax and Usage
`spanning-tree stp` *<STG number>* `vlan` *<VLAN number>* 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` *<STG number>* `vlan` *<VLAN number>* Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter. **Command mode:** Global configuration
`no spanning-tree stp` *<STG number>* `vlan all` Removes all VLANs from a Spanning Tree Group. **Command mode:** Global configuration
`spanning-tree stp` *<STG number or range>* `enable` Globally enables Spanning Tree Protocol. STG is turned on by default. **Command mode:** Global configuration
`no spanning-tree stp` *<STG number or range>* `enable` Globally disables Spanning Tree Protocol. **Command mode:** Global configuration

Table 188. RSTP/PVRST Configuration Options (continued)

Command Syntax and Usage
`default spanning-tree` *<STG number or range>* Restores a Spanning Tree instance to its default configuration. **Command mode:** Global configuration
`show spanning-tree stp` *<STG number or range>* Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See for details about the `information` parameter. **Command mode:** All

Bridge RSTP/PVRST Configuration

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

Table 189. Bridge Spanning Tree Configuration Options

Command Syntax and Usage
`spanning-tree stp` *<STG number or range>* `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 61440. **Command mode:** Global configuration
`spanning-tree stp` *<STG number or range>* `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. This command does not apply to MSTP. **Command mode:** Global configuration
`spanning-tree stp` *<STG number or range>* `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. This command does not apply to MSTP. **Command mode:** Global configuration

Table 189. Bridge Spanning Tree Configuration Options

Command Syntax and Usage
spanning-tree stp <*STG number or range*> 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. This command does not apply to MSTP **Command mode:** Global configuration
show spanning-tree [vlan <*VLAN ID*>] bridge Displays the current Spanning Tree parameters either globally or for a specific VLAN. See page 43 for sample output. **Command mode:** All

When configuring STG bridge parameters, the following formulas must be used:

- 2*(*fwd*-1) ≥ *mxage*
- 2*(*hello*+1) ≤ *mxage*

RSTP/PVRST Port Configuration

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 190. Spanning Tree Port Options

Command Syntax and Usage
spanning-tree stp <*STG number or range*> 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/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128. **Command mode:** Interface port
spanning-tree stp <*STG number or range*> 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: – 1Gbps = 20000 – 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

Table 190. Spanning Tree Port Options (continued)

Command Syntax and Usage

spanning-tree link-type {auto|p2p|shared}
 	
    Defines the type of link connected to the port, as follows:
 	
    – auto: Configures the port to detect the link type, and automatically match its settings.
    – p2p: Configures the port for Point-To-Point protocol.
    – shared: Configures the port to connect to a shared medium (usually a hub).
 	
    Command mode: Interface port

spanning-tree stp <*STG number or range*> enable
 	
    Enables STG on the port.
 	
    Command mode: Interface port

no spanning-tree stp <*STG number or range*> enable
 	
    Disables STG on the port.
 	
    Command mode: Interface port

show interface port <*port alias, number or range*> spanning-tree stp <*STG number or range*>
 	
    Displays the current STG port parameters.
 	
    Command mode: All

Forwarding Database Configuration

Use the following commands to configure the Forwarding Database (FDB).

Table 191. 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.
 	
    Command mode: Global configuration

show mac-address-table
 	
    Display current FDB configuration.
 	
    Command mode: All except User EXEC

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` *x*) (`flood-blocking`).

Use the following commands to configure static Multicast MAC entries in the Forwarding Database (FDB).

Table 192. Static Multicast MAC Configuration Options

Command Syntax and Usage
`mac-address-table multicast` *<MAC address>* *<VLAN number>* *<port alias, number or range>*
Adds 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 {all`|*<MAC address>* *<VLAN number>*`}`
Deletes a static multicast entry.
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 193. FDB Configuration Options

Command Syntax and Usage

`mac-address-table static <`*MAC address*`> port <`*system port number*`> vlan <`*VLAN number*`>`
    `{port <`*port alias or number*`>|portchannel <`*trunk number*`>|`
    `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*`>] port <`*system port number*`> [<`*VLAN number*`>]|all` Deletes permanent FDB entries. **Command mode**: Global configuration
`show mac-address-table` Display current FDB configuration. **Command mode**: All except User EXEC

ECP Configuration

Use the following commands to configure Edge Control Protocol (ECP).

Table 194. ECP Configuration Options

Command Syntax and Usage
`ecp retransmit-interval <`*100-9000*`>` Configures ECP retransmit interval in milliseconds. Default value is 1000. **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|upper-layer-protocols]` Displays settings for all ECP channels or registered ULPs. **Command mode**: All

LLDP Configuration

Use the following commands to configure Link Layer Detection Protocol (LLDP).

Table 195. LLDP Configuration Options

Command Syntax and Usage
`[no] lldp refresh-interval` *<5-32768>* Configures the message transmission interval, in seconds. The default value is 30. **Command mode**: Global configuration
`[no] 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
`lldp trap-notification-interval` *<1-3600>* Configures the trap notification interval, in seconds. The default value is 5. **Command mode**: Global configuration
`[no] lldp transmission-delay` *<1-8192>* Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port. The default value is 2. **Command mode**: Global configuration
`[no] 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. **Command mode**: Global configuration
`lldp enable` Globally turns LLDP on. The default setting is `on`. **Command mode**: Global configuration
`no lldp enable` Globally turns LLDP off. **Command mode**: Global configuration
`show lldp [port` *<port_number>*`]` Display current LLDP configuration. **Command mode**: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 196. 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: – Transmit only – Receive only – 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 197. Optional TLV Options

Command Syntax and Usage
`[no] lldp tlv portdesc` Enables or disables the Port 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 sysdescr` Enables or disables the System Description 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 mgmtaddr` Enables or disables the Management Address information type. **Command mode**: Interface port
`[no] lldp tlv portvid` Enables or disables the Port VLAN ID 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 vlanname` Enables or disables the VLAN Name 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 macphy` Enables or disables the MAC/Phy Configuration information type. **Command mode**: Interface port

Table 197. 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 linkaggr` Enables or disables the Link Aggregation 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 dcbx` Enables or disables the DCBX information type. **Command mode**: Interface port
`[no] lldp tlv all` Enables or disables all optional TLV information types. **Command mode**: Interface port
`show interface port` *<port alias or number>* `lldp` Display current LLDP port configuration. **Command mode**: All

Trunk Configuration

Trunk groups can provide super-bandwidth connections between RackSwitch G8124s or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. The maximum number of portchannels (static or dynamic) supported on the switch is 16You may use the numbers in the range 1-12 to configure static portchannels and the numbers in the range 13-36 to configure LACP portchannels, with the following restrictions:Up to 16 static trunk groups can be configured on the G8124, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 12 ports can belong to the same trunk group.
- You must configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-IBM devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 198. Trunk Configuration Options

Command Syntax and Usage
portchannel *<1-12>* port *<port alias or number>* Adds a physical port or ports to the current trunk group. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-). **Command mode:** Global configuration
no portchannel *<1-12>* port *<port alias or number>* Removes a physical port or ports from the current trunk group. **Command mode:** Global configuration
[no] portchannel *<1-12>* enable Enables or Disables the current trunk group. **Command mode:** Global configuration
no portchannel *<1-12>* Removes the current trunk group configuration. **Command mode:** Global configuration
show portchannel *<1-12>* Displays current trunk group parameters. **Command mode:** All

Trunk Hash Configuration

Use the following commands to configure trunk hash settings for the G8124. The trunk hash settings affect both static trunks and LACP trunks.

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 199 combined with the hash parameters listed in Table 200 and Table 216.

Table 199. Trunk Hash Options

Command Syntax and Usage
`show portchannel hash`
Display current trunk hash configuration.
Command mode: All

Trunk Hash Settings

Trunk hash parameters are set globally for the G8124. You can enable one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure trunk hash parameters for the G8124.

Table 200. Trunk Hash Settings

Command Syntax and Usage
`portchannel hash source-mac-address` Enable trunk hashing on the source MAC. **Command mode:** Global configuration
`portchannel hash destination-mac-address` Enable trunk hashing on the destination MAC. **Command mode:** Global configuration
`portchannel hash source-ip-address` Enable trunk hashing on the source IP. **Command mode:** Global configuration
`portchannel hash destination-ip-address` Enable trunk hashing on the destination IP. **Command mode:** Global configuration
`portchannel hash source-destination-ip` Enable trunk hashing on the source and destination IP. **Command mode:** Global configuration
`portchannel hash source-destination-mac` Enable trunk hashing on the source and destination MAC address. **Command mode:** Global configuration
`show portchannel hash` Display current trunk hash setting. **Command mode:** All

Virtual Link Aggregation Group Configuration

vLAG groups allow you to enhance redundancy and prevent implicit loops without using STP. The vLAG group acts as a single virtual entity for the purpose of establishing a multi-port trunk.

Table 201. vLAG Configuration Options

Command Syntax and Usage
`[no] vlag portchannel` *`<trunk group number>`* `enable` Enables or disables vLAG on the selected trunk group. **Command mode:** Global configuration
`[no] vlag adminkey` *`<1-65535>`* `enable` Enables or disables vLAG on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the vLAG configuration. **Command mode:** Global configuration
`[no] vlag enable` Enables or disables vLAG globally. **Command mode:** Global configuration
`[no] vlag tier-id` *`<1-512>`* Sets the vLAG peer ID.
`[no] 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
`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`. **Command mode:** Global configuration
`no vlag auto-recovery` Sets the auto-recovery timer to the default 300 seconds duration. **Command mode:** Global configuration
`vlag startup-delay` *`<0-3600>`* Sets, in seconds, the vLAG startup delay interval. The default value is `120`. **Command mode:** Global configuration

Table 201. vLAG Configuration Options

Command Syntax and Usage

`no vlag startup-delay`
 	
    Sets the vLAG startup-delay timer to the default 120 seconds duration.
 	
    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 202. vLAG Health Check Configuration Options

Command Syntax and Usage

`[no] 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 connect-retry-interval` *`<1-300>`*
 	
    Sets, in seconds, the vLAG health check connect retry interval. The default value is 30.
 	
    Command mode: Global configuration

`[no] 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-interval` *`<2-300>`*
 	
    Sets, in seconds, the time between vLAG keep alive attempts. The default value is 5.
 	
    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 203. vLAG ISL Configuration Options

Command Syntax and Usage
[no] vlag isl portchannel *<trunk number>* Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group. **Command mode:** Global configuration
[no] vlag isl adminkey *<1-65535>* Enables or disables vLAG Inter-Switch Link (ISL) on the selected LACP *admin key*. LACP trunks formed with this *admin key* will be included in the ISL. **Command mode:** Global configuration
show vlag Displays current vLAG parameters. **Command mode:** All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the G8124.

Table 204. Link Aggregation Control Protocol Options

Command Syntax and Usage
`lacp system-priority` *<1-65535>* Defines the priority value for the G8124. Lower numbers provide higher priority. The default value is 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 G8124's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP. **Command mode:** Global configuration
`no lacp` *<1-65535>* Deletes a selected LACP trunk, 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 205. LACP Port Options

Command Syntax and Usage
`lacp mode {off|active|passive}` Set the LACP mode for this port, as follows: – **off** Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is `off`. – **active** Turn LACP on and set this port to active. Active ports initiate LACPDUs. – **passive** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. **Command mode:** Interface port/Interface portchannel
`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
`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 trunk group. **Command mode:** Interface port/Interface portchannel
`[no] lacp suspend-individual` Enables or disables suspension of LACP individual mode, based on the lack of received LACPDU's. If enabled, the port is set in `suspended` state. If disabled, the port is allowed to become individual. The default value is `enabled`. **Command mode:** Interface port/Interface portchannel
`port-channel min-links <1-12>` Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the `down` state. **Command mode:** Interface port/Interface portchannel
`default lacp [key|mode|priority|suspend-individual]` Restores the selected parameters to their default values. **Command mode:** Interface port/Interface portchannel

Table 205. LACP Port Options

Command Syntax and Usage

`default port-channel min-links`
 	
    Restores the minimum number of links for this port to its default value.
 	
    Command mode: Interface port

`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 *IBM N/OS Application Guide*.

Table 206. Layer 2 Failover Configuration Options

Command Syntax and Usage

`failover enable`
 	
    Globally turns Layer 2 Failover `on`.
 	
    Command mode: Global configuration

`no failover enable`
 	
    Globally turns Layer 2 Failover `off`.
 	
    Command mode: Global configuration

`show failover trigger`
 	
    Displays current Layer 2 Failover parameters.
 	
    Command mode: All

Failover Trigger Configuration

Table 207. Failover Trigger Configuration Options

Command Syntax and Usage

[no] `failover trigger` *<1-8>* `enable`
 	
    Enables or disables the Failover trigger.
 	
    Command mode: Global configuration

`no failover trigger` *<1-8>*
 	
    Deletes 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

`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 208. Failover Manual Monitor Port Options

Command Syntax and Usage

`failover trigger` *<1-8>* `mmon monitor member` *<port alias or number>*
 	
    Adds the selected port to the Manual Monitor Port configuration.
 	
    Command mode: Global configuration

`no failover trigger` *<1-8>* `mmon monitor member` *<port alias or number>*
 	
    Removes the selected port from the Manual Monitor Port configuration.
 	
    Command mode: Global configuration

`failover trigger` *<1-8>* `mmon monitor portchannel` *<trunk number>*
 	
    Adds the selected trunk group to the Manual Monitor Port configuration.
 	
    Command mode: Global configuration

`no failover trigger` *<1-8>* `mmon monitor portchannel` *<trunk number>*
 	
    Removes the selected trunk group from the Manual Monitor Port configuration.
 	
    Command mode: Global configuration

Table 208. Failover Manual Monitor Port Options

Command Syntax and Usage
`failover trigger <1-8> mmon monitor adminkey <1-65535>` Adds an LACP *admin key* to the Manual Monitor Port configuration. LACP trunks 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 adminkey <1-65535>` Removes an LACP *admin key* from 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 209. Failover Manual Monitor Control Options

Command Syntax and Usage
`failover trigger <1-8> mmon control member <port alias or number>` Adds the selected port to the Manual Monitor Control configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon control member <port alias or number>` Removes the selected port from the Manual Monitor Control configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon control portchannel <trunk number>` Adds the selected trunk group to the Manual Monitor Control configuration. **Command mode:** Global configuration
`no failover trigger <1-8> mmon control portchannel <trunk number>` Removes the selected trunk group from the Manual Monitor Control configuration. **Command mode:** Global configuration
`failover trigger <1-8> mmon control adminkey <1-65535>` Adds an LACP *admin key* to the Manual Monitor Control configuration. LACP trunks formed with this admin key will be included in the Manual Monitor Control configuration. **Command mode:** Global configuration

Table 209. Failover Manual Monitor Control Options

Command Syntax and Usage
`no failover trigger` *<1-8>* `mmon control adminkey` *<1-65535>* Removes an LACP *admin key* from 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 *IBM N/OS 7.9 Application Guide*.

Table 210. 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 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` *<10-200>* Configures the FDB Update rate in packets per second. **Command mode:** Global configuration
`hotlinks enable` Globally enables Hot Links. **Command mode:** Global configuration
`no hotlinks enable` Globally disables Hot Links. **Command mode:** Global configuration
`show hotlinks` Displays current Hot Links parameters. **Command mode:** All

Hot Links Trigger Configuration

Table 211. Hot Links Trigger Configuration Options

Command Syntax and Usage
`hotlinks trigger <1-25> forward-delay <0-3600>` Configures the Forward Delay interval, in seconds. The default value is `1`. **Command mode:** Global configuration
`[no] 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> 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> enable` Enables or disables the Hot Links trigger. **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 212. Hot Links Master Configuration Options

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* master port *<port alias or number>* Adds or removes the selected port to the Hot Links Master interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* master portchannel *<trunk group number>* Adds or removes the selected trunk group to the Master interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* master adminkey *<1-65535>* Adds or removes an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* will be included in the 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 213. Hot Links Backup Configuration Options

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* backup port *<port alias or number>* Adds or removes the selected port to the Hot Links Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* backup portchannel *<trunk group number>* Adds or removes the selected trunk group to the Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* backup adminkey *<1-65535>* Adds or removes an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the 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 4094 VLANs can be configured on the G8124.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 214. VLAN Configuration Options

Command Syntax and Usage
vlan *<VLAN number>* Enter VLAN configuration mode. **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] shutdown Disables or enables local traffic on the specified VLAN. Default setting is enabled (no shutdown) **Command mode:** VLAN
stg *<STG number>* Assigns a VLAN to a Spanning Tree Group. **Note**: For MST no VLAN assignation is required. VLANs are mapped from CIST. **Command mode:** VLAN
[no] vmap *<1-127>* [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 number>* Deletes this VLAN. **Command mode:** VLAN
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.

Private VLAN Configuration

Use the following commands to configure Private VLANs.

Table 215. Private VLAN Options

Command Syntax and Usage
`[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
`[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
`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:
– `add` appends the secondary VLANs to the ones currently associated
– `remove` excludes the secondary VLANs from the ones currently associated
Command mode: VLAN
`show vlan private-vlan`
– Displays current parameters for the selected Private VLAN(s).
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 216. Layer 3 Configuration Commands

Command Syntax and Usage
`interface ip` *<interface number>* Configures the IP Interface. The G8124 supports up to 128 IP interfaces. However, IP interface 127 and 128 are reserved for switch management. To view command options, see page 310. **Command mode:** Global configuration
`route-map` {*<1-64>*} Enters IP Route Map mode. To view command options, see page 321. **Command mode:** Global configuration
`router rip` Enters the Routing Interface Protocol (RIP) configuration mode. To view command options, see page 325. **Command mode:** Global configuration
`router ospf` Enters OSPF configuration mode. To view command options, see page 329. **Command mode:** Global configuration
`ipv6 router ospf` Enters OSPFv3 configuration mode. To view command options, see page 340. **Command mode:** Global configuration
`router vrrp` Enters Virtual Router Redundancy (VRRP) configuration mode. To view command options, see page 385. **Command mode:** Global configuration
`ip pim component` *<1-2>* Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see page 394. **Command mode:** Global configuration
`ip router-id` *<IP address>* Sets the router ID. **Command mode:** Global configuration
`show layer3` Displays the current IP configuration. **Command mode:** All

IP Interface Configuration

The G8124 supports up to 128 IP interfaces. Each IP interface represents the G8124 on an IP subnet on your network. The Interface option is disabled by default.

Interface 127 and interface 128 are reserved for switch management, as follows:

- IF 127: Management port B
- IF 128: Management port A

Table 217. IP Interface Configuration Options

Command Syntax and Usage
`interface ip` *<interface number>* Enter IP interface mode. **Command mode:** Global configuration
`ip address` *<IP address>* `[`*<IP netmask>*`]` Configures the IP address of the switch interface, using dotted decimal notation. **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` *<IP address (such as 3001:0:0:0:0:0:abcd:12)>* `[anycast|enable|no enable]` Configures the IPv6 address of the switch interface, using hexadecimal format with colons. **Command mode:** Interface IP
`ipv6 secaddr6 address` *<IP address (such as 3001:0:0:0:0:0:abcd:12)>* *<prefix length>* `[anycast]` Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons. **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
`vlan` *<VLAN number>* 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. **Command mode:** Interface IP

Table 217. IP Interface Configuration Options (continued)

Command Syntax and Usage
[no] relay Enables or disables the BOOTP relay on this interface. 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] ipv6 unreachables Enables or disables sending of ICMP Unreachable messages. The default setting is enabled. **Command mode:** Interface IP
enable Enables this IP interface. **Command mode:** Interface IP
no enable Disables this IP interface. **Command mode:** Interface IP
no interface ip *<interface number>* Removes this IP interface. **Command mode:** Interface IP
show interface ip *<interface number>* Displays the current interface settings. **Command mode:** All

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery configuration commands.

Table 218. IPv6 Neighbor Discovery Configuration Options

Command Syntax and Usage
[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
[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
`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 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 reachable-time` *<1-3600>* [no] `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 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

Table 218. IPv6 Neighbor Discovery Configuration Options (continued)

Command Syntax and Usage
[no] ipv6 nd ra-intervalmin *<3-1800>* 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 retransmit-time *<0-4294967>* [no] 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 hops-limit *<0-255>* Configures the Router Advertisement hop limit. The default value is 64. **Command mode:** Interface IP
[no] ipv6 nd advmtu Enables or disables the MTU option in Router Advertisements. The default setting is enabled. **Command mode:** Interface IP

Default Gateway Configuration

The switch can be configured with up to four IPv4 gateways, as follows:

- Gateway 1 and Gateway 2: data traffic
- Gateway 3: Management port A
- Gateway 4: Management port B

This option is disabled by default.

Table 219. IPv4 Default Gateway Options

Command Syntax and Usage
`ip gateway` *<1-4>* `address` *<IP address>* Configures the IP address of the default IP gateway using dotted decimal notation. **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. 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. The default is 8 attempts. **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`. The `arp` option does not apply to management gateways. **Command mode:** Global configuration
`ip gateway` *<1-4>* `enable` Enables the gateway for use. **Command mode:** Global configuration
`no ip gateway` *<1-4>* `enable` Disables the gateway. **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 220. IPv4 Static Route Configuration Options

Command Syntax and Usage
`ip route` *\<IP subnet\> \<IP netmask\> \<IP nexthop\>* [*\<interface 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\>* [*\<interface number\>*] Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation. **Command mode:** Global configuration
`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

`ip route ecmphash [sip][dip][protocol][tcpl4][udpl4]`
`[sport][dport]`
 	
Configures ECMP hashing parameters. You may choose one or more of the following parameters:
 	
– `sip`: Source IP address
– `dip`: Destination IP address
– `protocol`: Layer 3 protocol
– `tcpl4`: Layer 4 TCP traffic
– `udpl4`: Layer 4 UDP traffic
– `sport`: Source port
– `dport`: Destination port
 	
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

Table 220. IPv4 Static Route Configuration Options (continued)

Command Syntax and Usage
`ip route retries` *<1-60>*   Configures the number of ECMP health-check retries. The default value is 3. **Command mode:** Global configuration
`[no] ip route healthcheck` Enables or disables static route health checks. The default setting is `disabled`. **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 must be enabled, and the required VLANs must be added to IGMP Snooping.

Table 221. IP Multicast Route Configuration Commands

Command Syntax and Usage
ip mroute *<IPMC destination>* *<VLAN number>* *<port alias or number>*] Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified. **Command mode:** Global configuration
no ip mroute *<IPMC destination>* *<VLAN number>* *<port alias or number>* [*<virtual router ID>*] Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified. **Command mode:** Global configuration
ip mroute *<IP address>* *<VLAN number>* portchannel *<trunk group number>* [*<virtual router ID>*] Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified. **Command mode:** Global configuration
no ip mroute *<IP address>* *<VLAN number>* portchannel *<trunk group number>* [*<virtual router ID>*] Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified. **Command mode:** Global configuration
ip mroute *<IP address>* *<VLAN number>* adminkey *<1-65535>* [*<virtual router ID>*|none] Adds 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 *<IP address>* *<VLAN number>* adminkey *<1-65535>* [*<virtual router ID>*|none] Removes a static multicast route. The destination address, VLAN, and LACP *admin key* of the route to remove must be specified. **Command mode:** Global configuration

Table 221. IP Multicast Route Configuration Commands

Command Syntax and Usage
`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 except User EXEC

ARP Configuration

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. 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 222. 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 except User EXEC

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 223. ARP Static Configuration Options

Command Syntax and Usage
ip arp *<IP address>* *<MAC address>* vlan *<vlan number>* port *<port alias or number>* Adds a permanent ARP entry. **Command mode:** Global configuration
no ip arp *<IP address>* Deletes a permanent ARP entry. **Command mode:** Global configuration
no ip arp all Deletes all static ARP entries. **Command mode:** Global configuration
show ip arp static Displays current static ARP configuration. **Command mode:** All

IP Forwarding Configuration

Table 224. IP Forwarding Configuration Options

Command Syntax and Usage
[no] ip routing directed-broadcasts Enables or disables forwarding directed broadcasts. 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
[no] ip routing icmp6-redirect Enables or disables IPv6 ICMP re-directs. The default setting is disabled. **Command mode:** Global configuration

Table 224. IP Forwarding Configuration Options

Command Syntax and Usage
`ip routing` Enables IP forwarding (routing) on the G8124. Forwarding is turned on by default. **Command mode:** Global configuration
`no ip routing` Disables IP forwarding (routing) on the G8124. **Command mode:** Global configuration
`show ip routing` Displays the current IP forwarding settings. **Command mode:** All except User EXEC

Network Filter Configuration

Table 225. 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.
`ip match-address` *<1-256>* `enable` Enables the Network Filter configuration. **Command mode:** Global configuration
`no ip match-address` *<1-256>* `enable` 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 except User EXEC

Routing Map Configuration

Note: The *map number* (1-*64*) represents the routing map you wish to configure.

Routing maps control and modify routing information.

Table 226. Routing Map Configuration Options

Command Syntax and Usage
`route-map` *<1-64>* Enter route map configuration mode. **Command mode:** Global configuration
[no] `access-list` *<1-8>* Configures the Access List. **Command mode:** Route map For more information, see .
[no] `as-path-list` *<1-8>* Configures the Autonomous System (AS) Filter. **Command mode:** Route map For more information, see .
[no] `as-path-preference` *<1-65535>* Sets the AS path preference of the matched route. You can configure up to three path preferences. **Command mode:** Route map
[no] `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] `metric` *<1-4294967294>* Sets the metric of the matched route. **Command mode:** Route map
[no] `metric-type` {1|2} Assigns the type of OSPF metric. The default is type 1. – **Type 1**—External routes are calculated using both internal and external metrics. – **Type 2**—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2. – `none`—Removes the OSPF metric. **Command mode:** Route map
`precedence` *<1-255>* Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10. **Command mode:** Route map

Table 226. Routing Map Configuration Options (continued)

Command Syntax and Usage
[no] weight *<0-65534>* Sets the weight of the route map. **Command mode:** Route map
[no] 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. None removes the community attribute from prefix that passed the route-map. Use the no form of the command to remove the entry. **Command mode:** Route map
enable Enables the route map. **Command mode:** Route map
no enable Disables the route map. **Command mode:** Route map
no route-map *<1-64>* Deletes the route map. **Command mode:** Route map
show route-map [*<1-64>*] Displays the current route configuration. **Command mode:** All except User EXEC

IP Access List Configuration

Note: The *route map number (*1-64) and the *access list number* (1-8) represent the IP access list you wish to configure.

Table 227. IP Access List Configuration Options

Command Syntax and Usage
[no] `access-list` *<1-8>* `match-address` *<1-256>*   Sets the network filter number.   **Command mode:** Route map   See "Network Filter Configuration" on page 320 for details.
[no] `access-list` *<1-8>* `metric` *<1-4294967294>*   Sets the metric value in the AS-External (ASE) LSA.   **Command mode:** Route map
`access-list` *<1-8>* `action` {`permit`|`deny`}   Permits or denies action for the access list.   **Command mode:** Route map
`access-list` *<1-8>* `enable`   Enables the access list.   **Command mode:** Route map
`no access-list` *<1-8>* `enable`   Disables the access list.   **Command mode:** Route map
`no access-list` *<1-8>*   Deletes the access list.   **Command mode:** Route map
`show route-map` *<1-64>* `access-list` *<1-8>*   Displays the current Access List configuration.   **Command mode:** All

Autonomous System Filter Path Configuration

Note: The *rmap number* and the *path number* represent the AS path you wish to configure.

Table 228. AS Filter Configuration Options

Command Syntax and Usage
`as-path-list` *<1-8>* `as-path` *<1-65535>*   Sets the Autonomous System filter's path number. **Command mode:** Route map
`as-path-list` *<1-8>* `action {permit|deny}` Permits or denies Autonomous System filter action. **Command mode:** Route map
`as-path-list` *<1-8>* `enable` Enables the Autonomous System filter. **Command mode:** Route map
`no as-path-list` *<1-8>* `enable` 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` *<1-64>* `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 229. Routing Information Protocol Options

Command Syntax and Usage
`router rip`   Enter Router RIP configuration mode.   **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
`enable`   Globally turns RIP `on`.   **Command mode:** Router RIP
`no enable`   Globally turns RIP `off`.   **Command mode:** Router RIP
`show ip rip`   Displays the current RIP configuration.   **Command mode:** All except User EXEC

Routing Information Protocol 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 230. RIP Interface Options

Command Syntax and Usage
`ip rip version {1|2|both}` Configures the RIP version used by this interface. The default value is version 2. **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 listen` When enabled, the switch learns routes from other routers. 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 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
`[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 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. When disabled, the switch rejects RIP default routes. The default value is `none`. **Command mode:** Interface IP

Table 230. RIP Interface Options (continued)

Command Syntax and Usage
[no] 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 authentication type [*<password>*] Configures the authentication type. The default is none. **Command mode:** Interface IP
[no] ip rip authentication key *<password>* Configures the authentication key password. **Command mode:** Interface IP
ip rip enable Enables this RIP interface. **Command mode:** Interface IP
no ip rip enable Disables this RIP interface. **Command mode:** Interface IP
show interface ip *<interface number>* rip Displays the current RIP configuration. **Command mode:** All

RIP Route Redistribution Configuration

The following table describes the RIP Route Redistribution commands.

Table 231. RIP Redistribution Options

Command Syntax and Usage
`redistribute {fixed|static|ospf|eospf|ebgp|ibgp}` *<1-64>* Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (,). To add all 64 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
`no redistribute {fixed|static|ospf|eospf|ebgp|ibgp}` *<1-64>* Removes the route map from the RIP route redistribution list. To remove specific route maps, enter routing map numbers, separated by a comma (,). To remove all 64 route maps, type `all`. **Command mode:** Router RIP
`redistribute {fixed|static|ospf|eospf|ebgp|ibgp} export` *<1-15>* Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`. **Command mode:** Router RIP
`show ip rip redistribute` Displays the current RIP route redistribute configuration. **Command mode:** All

Open Shortest Path First Configuration

Table 232. OSPF Configuration Options

Command Syntax and Usage

`router ospf`
 	
    Enter Router OSPF configuration mode.
 	
    Command mode: Global configuration

`area-range` *<1-16>*
 	
    Configures summary routes for up to 16 IP addresses. See to view command options.
 	
    Command mode: Router OSPF

`ip ospf` *<1-128>*
 	
    Configures the OSPF interface. See to view command options.
 	
    Command mode: Interface IP

`area-virtual-link` *<1-3>*
 	
    Configures the Virtual Links used to configure OSPF for a Virtual Link. See to view command options.
 	
    Command mode: Router OSPF

`message-digest-key` *<1-255>* `md5-key` *<text string>*
 	
    Assigns a string to MD5 authentication key.
 	
    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 to view command options.
 	
    Command mode: Router OSPF

`lsdb-limit` *<LSDB limit (0-9216, 0 for no limit)>*
 	
    Sets the link state database limit.
 	
    Command mode: Router OSPF

`[no] default-information` *<1-16777214>* {*<AS external metric type (1-2)>*}
 	
    Sets one default route among multiple choices in an area. Use `none` for no default.
 	
    Command mode: Router OSPF

Table 232. OSPF Configuration Options (continued)

Command Syntax and Usage

`enable`
 	
    Enables OSPF on the G8124.
 	
    Command mode: Router OSPF

`no enable`
 	
    Disables OSPF on the G8124.
 	
    Command mode: Router OSPF

`show ip ospf`
 	
    Displays the current OSPF configuration settings.
 	
    Command mode: All except User EXEC

Area Index Configuration

Table 233. 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>* 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. – **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. – **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. – **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
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. Metric type determines the method for influencing routing decisions for external routes. **Command mode:** Router OSPF
[no] area *<0-19>* authentication-type {password|md5} **None:** No authentication required. **Password:** Authenticates simple passwords so that only trusted routing devices can participate. **MD5:** This parameter is used when MD5 cryptographic authentication is required. **Command mode:** Router OSPF
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>* enable Enables the OSPF area. **Command mode:** Router OSPF

Table 233. Area Index Configuration Options (continued)

Command Syntax and Usage

`no area` *<0-19>* `enable`
 	
    Disables the OSPF area.
 	
    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 except User EXEC

OSPF Summary Range Configuration

Table 234. 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 G8124. **Command mode:** Router OSPF
`[no] area-range <1-16> hide` Hides the OSPF summary range. **Command mode:** Router OSPF
`area-range <1-16> enable` Enables the OSPF summary range. **Command mode:** Router OSPF
`no area-range <1-16> enable` Disables 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:** Router OSPF

OSPF Interface Configuration

Table 235. OSPF Interface Configuration Options

Command Syntax and Usage
`ip ospf area` *<0-19>* Configures the OSPF area index. **Command mode:** Interface IP
`ip ospf priority` *<0-255>* Configures the priority value for the G8124'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 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 hello-interval` *<1-65535>* `ip ospf hello-interval` *<50-65535ms>* Configures the interval, in seconds or milliseconds, between the `hello` packets for the interfaces. **Command mode:** Interface IP
`ip ospf dead-interval` *<1-65535>* `ip ospf dead-interval` *<1000-65535ms>* Configures the health parameters of a `hello` packet, in seconds or milliseconds, before declaring a silent router to be down. **Command mode:** Interface IP
`ip ospf transit-delay` *<1-3600>* Configures the transit delay in seconds. **Command mode:** Interface IP
`ip ospf retransmit-interval` *<1-3600>* Configures the retransmit interval in seconds. **Command mode:** Interface IP
[no] `ip ospf key` *<key string>* Sets the authentication key to clear the password. **Command mode:** Interface IP

Table 235. OSPF Interface Configuration Options (continued)

Command Syntax and Usage

[no] ip ospf message-digest-key *<1-255>*
 	
    Assigns an MD5 key to the interface.
 	
    Command mode: Interface IP

[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 enable
 	
    Enables OSPF interface.
 	
    Command mode: Interface IP

no ip ospf enable
 	
    Disables OSPF interface.
 	
    Command mode: Interface IP

no ip ospf
 	
    Deletes the OSPF interface.
 	
    Command mode: Interface IP

Show interface ip *<interface number>* ospf
 	
    Displays the current settings for OSPF interface.
 	
    Command mode: All except User EXEC

OSPF Virtual Link Configuration

Table 236. 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>* `hello-interval` *<1-65535>* `area-virtual-link` *<1-3>* `hello-interval` *<50-65535ms>* 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>* `dead-interval` *<1-65535>* `area-virtual-link` *<1-3>* `dead-interval` *<1000-65535ms>* Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 40 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 one second. **Command mode:** Router OSPF
`area-virtual-link` *<1-3>* `retransmit-interval` *<1-3600>* Configures the retransmit interval, in seconds. The default value is five seconds. **Command mode:** Router OSPF
`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
[no] `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
`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
`area-virtual-link` *<1-3>* `enable` Enables OSPF virtual link. **Command mode:** Router OSPF

Table 236. OSPF Virtual Link Configuration Options (continued)

Command Syntax and Usage
`no area-virtual-link <1-3> enable` Disables OSPF virtual link. **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 except User EXEC

OSPF Host Entry Configuration

Table 237. 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
host *<1-128>* enable Enables OSPF host entry. **Command mode:** Router OSPF
no host *<1-128>* enable Disables 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 except User EXEC

OSPF Route Redistribution Configuration

.

Table 238. OSPF Route Redistribution Configuration Options

Command Syntax and Usage
`redistribute {fixed|static|rip|ebgp|ibgp}` *<rmap ID (1-64)>* Adds 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
`no redistribute {fixed|static|rip|ebgp|ibgp}` *<rmap ID (1-64)>* Removes the route map from the route redistribution list. Removes routing maps from the `rmap` list. **Command mode:** Router OSPF
`[no] redistribute {fixed|static|rip|ebgp|ibgp} export metric` *<1-16777214>* `metric-type {type1|type2}` Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`. **Command mode:** Router OSPF
`show ip ospf redistribute` Displays the current route map settings. **Command mode:** All except User EXEC

OSPF MD5 Key Configuration

Table 239. 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 except User EXEC

Open Shortest Path First Version 3 Configuration

Table 240. OSPFv3 Configuration Options

Command Syntax and Usage
`[no] ipv6 router ospf` Enter OSPFv3 configuration mode. Enables or disables OSPFv3 routing protocol. **Command mode**: Global configuration
`abr-type [standard|cisco|ibm]` Configures the Area Border Router (ABR) type, as follows: – Standard – Cisco – IBM The default setting is `standard`. **Command mode**: Router OSPF3
`as-external lsdb-limit` *<LSDB limit (0-2147483647, -1 for no limit)>* Sets the link state database limit. **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 (zero). **Command mode**: Router OSPF3

`neighbor` *<1-256>* `{address` *<IPv6 address>*`|enable|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.
– `address` configures the neighbor's IPv6 address
– `enable` activates a previously disabled neighbor
– `interface` configures the OSPFv3 interface used for the neighbor entry
– `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. The default value is 1.
 	
Command mode: Router OSPF3

`no neighbor` *<1-256>* `[enable]` Deletes the neighbor entry. Using the `enable` option only disables the neighbor, while preserving it's settings. **Command mode**: Router OSPF3

Table 240. OSPFv3 Configuration Options (continued)

Command Syntax and Usage
`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
`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. Configures the number of seconds between SPF calculations. The default value is 10. **Command mode**: Router OSPF3
`router-id` *<IPv4 address>* Defines the router ID. **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
`enable` Enables OSPFv3 on the switch. **Command mode**: Router OSPF3
`no enable` Disables OSPFv3 on the switch. **Command mode**: Router OSPF3
`show ipv6 ospf` Displays the current OSPF configuration settings. **Command mode**: All

OSPFv3 Area Index Configuration

Table 241. OSPFv3 Area Index Configuration Options

Command Syntax and Usage
area *<area index>* `area-id` *<IP address>* Defines the IP address of the OSPFv3 area number. **Command mode**: Router OSPF3
area *<area index>* `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. **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. **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. **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. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas. Enables or disables 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
area *<area index>* `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 *<area index>* `default-metric type` *<1-3>* Configures the default metric type applied to the route. This command applies only to area type of Stub/NSSA. **Command mode**: Router OSPF3
area *<area index>* `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. **Command mode**: Router OSPF3

Table 241. OSPFv3 Area Index Configuration Options (continued)

Command Syntax and Usage
`area ⟨area index⟩ translation-role always│candidate` Configures the translation role for an NSSA area, as follows: – Always: Type 7 LSAs are always translated into Type 5 LSAs. – Candidate: An NSSA border router participates in the translator election process. The default setting is `candidate`. **Command mode**: Router OSPF3
`area ⟨area index⟩ enable` Enables the OSPF area. **Command mode**: Router OSPF3
`area ⟨area index⟩ no enable` Disables the OSPF area. **Command mode**: Router OSPF3
`no area ⟨area index⟩` Deletes the OSPF area. **Command mode**: Router OSPF3
`show ipv6 ospf areas` Displays the current OSPFv3 area configuration. **Command mode**: All

OSPFv3 Summary Range Configuration

Table 242. 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
area-range *<1-16>* lsa-type summary|Type7 Configures the LSA type, as follows: – Summary LSA – 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>* hide Hides the OSPFv3 summary range. **Command mode**: Router OSPF3
area-range *<1-16>* enable Enables the OSPFv3 summary range. **Command mode**: Router OSPF3
area-range *<1-16>* no enable Disables the OSPFv3 summary range. **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

Table 243. 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>* `area` *<area index (0-2)>* Configures the area index used by the switch. **Command mode**: Router OSPF3
`summary-prefix` *<1-16>* `aggregation-effect` {`allowAll`|`denyAll`|`advertise`|`not-advertise`} Configures the aggregation effect, as follows: – `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. – `denyAll`: Type-5 and Type-7 LSAs are not generated. – `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. – `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
[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
`summary-prefix` *<1-16>* `enable` Enables the OSPFv3 AS-external range. **Command mode**: Router OSPF3
`summary-prefix` *<1-16>* `no enable` 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

Table 244. OSPFv3 Interface Configuration Options

Command Syntax and Usage
`interface ip` *<interface number>* Enter Interface IP mode, from Global Configuration mode. **Command mode**: Global configuration
`ipv6 ospf area` *<area index (0-2)>* Configures the OSPFv3 area index. **Command mode**: Interface IP
`ipv6 ospf area` *<area index (0-2)>* `instance` *<0-255>* Configures the instance ID for the interface. **Command mode**: Interface IP
`[no] 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). **Command mode**: Interface IP
`[no] ipv6 ospf cost` *<1-65535>* Configures the metric value for sending a packet on the interface. **Command mode**: Interface IP
`[no] 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 linklsasuppress` Enables or disables Link LSA suppression. When suppressed, no Link LSAs are originated. Default setting is disabled. **Command mode**: Interface IP

Table 244. OSPFv3 Interface Configuration Options (continued)

Command Syntax and Usage
`ipv6 ospf network {broadcast|non-broadcast|pint-to-multipoint| point-to-point}` Configures the network type for the OSPFv3 interface: – `broadcast`: network where all routers use the broadcast capability – `non-broadcast`: non-broadcast multiple access (NBMA) network supporting pseudo-broadcast (multicast and broadcast traffic is configured manually) – `point-to-multipoint`: network where multiple point-to-point links are set up on the same interface – `point-to-point`: network that joins a single pair of routers The default value is `broadcast`. **Command mode**: Interface IP
`ipv6 ospf poll-interval` *<0-4294967295>* Configures the poll interval in seconds for neighbors in NBMA networks. Default value is 120. **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
`[no] 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 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 retransmit-interval` *<1-1800>* Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface. **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 enable` Enables OSPFv3 on the interface. **Command mode**: Interface IP

Table 244. OSPFv3 Interface Configuration Options (continued)

Command Syntax and Usage
`ipv6 ospf no enable` Disables OSPFv3 on the interface. **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**: Interface IP

OSPFv3 over IPSec Configuration

The following table describes the OSPFv3 over IPsec Configuration commands.

Table 245. Layer 3 IPsec Configuration Options

Command Syntax and Usage
`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: – MD5 (hexadecimal key length is 32) – SHA1 (hexadecimal key length is 40) **Command mode:** Interface IP
`[no] ipv6 ospf authentication ipsec enable` Enables or disables IPsec. **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

Table 245. Layer 3 IPsec Configuration Options (continued)

Command Syntax and Usage

`ipv6 ospf encryption ipsec spi` *<256-4294967295>*
   `esp` {`3des`|`aes-cbc`|`des`|`null`} *<encryption key (hexadecimal)>*|`null`}
   {`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:
– 3DES (hexadecimal key length is 48)
– AES-CBC (hexadecimal key length is 32)
– DES (hexadecimal key length is 16)
 	
The authentication algorithms supported are:
– MD5 (hexadecimal key length is 32)
– SHA1 (hexadecimal key length is 40)
– none
 	
Note: If the encryption algorithm is null, the authentication algorithm must be either MD5 or SHA1. (hexadecimal key length is 40). If an encryption algorithm is specified (3DES, AES-CBC, or DES), the authentication algorithm can be none.
 	
Command mode: Interface IP

`ipv6 ospf encryption ipsec enable` Enables OSPFv3 encryption for this interface. **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

Table 246. OSPFv3 Virtual Link Configuration Options

Command Syntax and Usage
`area-virtual-link` *<1-3>* `area` *<area index (0-2)>* Configures the OSPF area index. **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>* `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
`area-virtual-link` *<1-3>* `transmit-delay` *<1-1800>* Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. **Command mode**: Router OSPF3
`area-virtual-link` *<1-3>* `retransmit-interval` *<1-1800>* Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds. **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>* `enable` Enables OSPF virtual link. **Command mode**: Router OSPF3
`area-virtual-link` *<1-3>* `no enable` Disables OSPF virtual link. **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 247. Layer 3 IPsec Configuration Options

Command Syntax and Usage
`area-virtual-link <1-3> authentication ipsec {default｜enable｜spi <256-4294967295>}` Sets OSPFv3 authentication mode. **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
`area-virtual-link <1-3> encryption ipsec {default｜enable｜spi <256-4294967295>}` Sets OSPFv3 encryption. **Command mode:** Router OSPF3
`area-virtual-link <1-3> encryption ipsec spi <256-4294967295> esp {3des <3des key>｜aes-cbc <aes-cbc key>｜null} {md5｜none｜sha1}` Configures the OSPFv3 security parameter index encryption. **Command mode:** Router OSPF3

OSPFv3 Host Entry Configuration

Table 248. 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 <area index (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
`host <1-128> enable` Enables the host entry. **Command mode**: Router OSPF3

Table 248. OSPFv3 Host Entry Configuration Options

Command Syntax and Usage
`no host <1-128> enable` 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

Table 249. 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
`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> metric-type asExttype1|asExttype2` Configures the metric type applied to the route before it is advertised into the OSPFv3 domain. **Command mode**: Router OSPF3
`[no] redist-config <1-128> tag <0-4294967295>` Configures the route tag. **Command mode**: Router OSPF3
`redist-config <1-128> enable` Enables the OSPFv3 redistribution entry. **Command mode**: Router OSPF3
`no redist-config <1-128> enable` Disables the OSPFv3 redistribution entry. **Command mode**: Router OSPF3

Table 249. OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage
`no redist-config <`*1-128*`>` Deletes the OSPFv3 redistribution entry. **Command mode**: Router OSPF3
`show ipv6 ospf redist-config` Displays the current OSPFv3 redistribution configuration entries. **Command mode**: Router OSPF3

OSPFv3 Redistribute Configuration

Table 250. OSPFv3 Redistribute Configuration Options

Command Syntax and Usage

`[no] 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. To remove a previous configuration and stop exporting the routes of the protocol, use the `no` form of the command.
 	
Command mode: Router OSPF3

`show ipv6 ospf` Displays the current OSPFv3 route redistribution settings. **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 251. BGP Peer Configuration Options

Command Syntax and Usage
neighbor *<peer number>* 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 *<peer number>* remote-as *<1-65535>*   Sets the remote autonomous system number for the specified peer.   **Command mode:** Router BGP
[no] neighbor *<peer number>* 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 *<peer number>* send-community   Enables or disables sending a community attribute to a BGP neighbor.   **Command mode:** Router BGP
neighbor *<peer number>* update-source {*<interface number>*|loopback *<1-5>*}   Sets the source interface number for this peer.   **Command mode:** Router BGP
neighbor *<peer number>* 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 *<peer number>* timers keep-alive *<0, 1-21845>*   Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.   **Command mode:** Router BGP
neighbor *<peer number>* advertisement-interval *<1-65535>*   Sets time, in seconds, between advertisements. The default value is 60 seconds.   **Command mode:** Router BGP
neighbor *<peer number>* retry-interval *<1-65535>*   Sets connection retry interval, in seconds. The default value is 120 seconds.   **Command mode:** Router BGP

Table 251. BGP Peer Configuration Options (continued)

Command Syntax and Usage
`neighbor <peer number> route-origination-interval <1-65535>` Sets the minimum time between route originations, in seconds. The default value is 15 seconds. **Command mode:** Router BGP
`neighbor <peer number> 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 <peer number> time-to-live` Disables the TTL feature. **Command mode:** Router BGP
`neighbor <peer number> ttl-security hops <1-254>` Sets the minimum number of time-to-live (TTL) router hops an IP packet must make to not be discarded. **Command mode:** Router BGP
`no neighbor <peer number> ttl-security hops` Disables the TTL security feature. **Command mode:** Router BGP
`neighbor <peer number> route-map in <1-64>` Adds route map into in-route map list. **Command mode:** Router BGP
`neighbor <peer number> route-map out <1-64>` Adds route map into out-route map list. **Command mode:** Router BGP
`no neighbor <peer number> route-map in <1-64>` Removes route map from in-route map list. **Command mode:** Router BGP
`no neighbor <peer number> route-map out <1-64>` Removes route map from out-route map list. **Command mode:** Router BGP

Table 251. BGP Peer Configuration Options (continued)

Command Syntax and Usage
`no neighbor` *<peer number>* `shutdown` Enables this peer configuration. **Command mode:** Router BGP
`neighbor` *<peer number>* `shutdown` Disables this peer configuration. **Command mode:** Router BGP
`no neighbor` *<peer number>* Deletes this peer configuration. **Command mode:** Router BGP
`[no] neighbor` *<peer number>* `password` *<1-16 characters>* Configures the BGP peer password. **Command mode:** Router BGP
`[no] neighbor` *<peer number>* `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
`show ip bgp neighbor` [*<peer number>*] Displays the current BGP peer configuration. **Command mode:** All
`neighbor` *<peer number>* `next-hop-self` Enforces using the router's own IP address as next-hop attribute when sending BGP updates to the peer. Applicable only for EBGP routes. **Command mode:** Router BGP
`no neighbor` *<peer number>* `next-hop-self` Doesn't enforce using the router's own IP address as next-hop attribute when sending BGP updates to the peer. **Command mode:** Router BGP

BGP Neighbor Redistribution Configuration

This menu enables you to redistribute routes learned from various routing information sources into BGP.

Table 252. BGP Neighbor Redistribution Configuration Options

Command Syntax and Usage
[no] neighbor *<peer number>* redistribute default-metric *<1-4294967294>*   Sets default metric of advertised routes.   **Command mode:** Router BGP
[no] neighbor *<peer number>* redistribute default-action {import|originate|redistribute}   Sets default route action.   Defaults routes can be configured as import, originate, redistribute, or none.   **None:** No routes are configured   **Import:** Import these routes.   **Originate:** The switch sends a default route to peers if it does not have any default routes in its routing table.   **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 *<peer number>* redistribute rip   Enables or disables advertising RIP routes.   **Command mode:** Router BGP
[no] neighbor *<peer number>* redistribute ospf   Enables or disables advertising OSPF routes.   **Command mode:** Router BGP
[no] neighbor *<peer number>* redistribute fixed   Enables or disables advertising fixed routes.   **Command mode:** Router BGP
[no] neighbor *<peer number>* redistribute static   Enables or disables advertising static routes.   **Command mode:** Router BGP
show ip bgp neighbor *<peer number>* redistribute   Displays current redistribution configuration.   **Command mode:** All except User EXEC

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 253. BGP Peering Group Configuration Options

Command Syntax and Usage
[no] neighbor group *<group number>* name *<1-32 characters>*   Sets the name for the group.   **Command mode:** Router BGP
neighbor group *<group number>* 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 *<group number>* remote-as *<AS number (1-65535)>* [alternate-as *<AS number (1-65535)>*]   Adds a remote access server (RAS) into the RAS list.   **Command mode:** Router BGP
[no] neighbor group *<group number>* 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 *<group number>* send-community   Enables or disables sending a community attribute to a BGP neighbor group.   **Command mode:** Router BGP
neighbor group *<group number>* listen limit *<group limit (1-96)>*   Sets the maximum number of BGP dynamic peers.   **Command mode:** Router BGP
neighbor group *<group number>* update-source *<interface number (1-126)>*   Sets the local IP interface.   **Command mode:** Router BGP
neighbor group *<group number>* update-source loopback *<interface number (1-5)>*   Sets the loopback interface number for this peering group.   **Command mode:** Router BGP

Table 253. BGP Peering Group Configuration Options (continued)

Command Syntax and Usage
`neighbor group` *<group number>* `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. **Command mode:** Router BGP
`neighbor group` *<group number>* `timers keep-alive` *<keepalive time (0, 1-21845)>* Sets the keep-alive time for the specified peering group in seconds. The default value is 60. **Command mode:** Router BGP
`neighbor group` *<group number>* `advertisement-interval` *<min adv time (1-65535)>* Sets time, in seconds, between advertisements. The default value is 60 seconds. **Command mode:** Router BGP
`neighbor group` *<group number>* `route-origin-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
`neighbor group` *<group number>* `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` *<group number>* `time-to-live` *<1-255>* Disables the TTL feature. **Command mode:** Router BGP
`neighbor group` *<group number>* `ttl-security hops` *<1-254>* Sets the minimum number of time-to-live (TTL) router hops an IP packet must make to not be discarded. **Command mode:** Router BGP

Table 253. BGP Peering Group Configuration Options (continued)

Command Syntax and Usage
`no neighbor group` *\<group number\>* `ttl-security hops` Disables the TTL security feature. **Command mode:** Router BGP
`neighbor group` *\<group number\>* `route-map in` *\<route map ID (1-64)\>* Adds route map into in-route map list. **Command mode:** Router BGP
`neighbor group` *\<group number\>* `route-map out` *\<route map ID (1-64)\>* Adds route map into out-route map list. **Command mode:** Router BGP
`[no] neighbor group` *\<group number\>* `route-map in` *\<route map ID (1-64)\>* Removes route map from in-route map list. **Command mode:** Router BGP
`[no] neighbor group` *\<group number\>* `route-map out` *\<route map ID (1-64)\>* Removes route map from out-route map list. **Command mode:** Router BGP
`[no] neighbor group` *\<group number\>* `password` Configures the BGP peer password. **Command mode:** Router BGP
`[no] neighbor group` *\<group number\>* `shutdown` Enables this peering group configuration. **Command mode:** Router BGP
`neighbor group` *\<group number\>* `shutdown` Disables this peering group configuration. **Command mode:** Router BGP
`no [no] neighbor group` *\<group number\>* Deletes this peering group configuration. **Command mode:** Router BGP
`neighbor group` *\<group number\>* `next-hop-self` Enforces using 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

Table 253. BGP Peering Group Configuration Options (continued)

Command Syntax and Usage
`no neighbor group` <*group number*> `next-hop-self` Doesn't enforce using the router's own IP address as next-hop attribute when sending BGP updates to the peering group. **Command mode:** Router BGP
`show ip bgp neighbor group` [<*neighbor group number*>] Displays the current peering group configuration. **Command mode:** All

BGP Neighbor Redistribution Configuration

This menu enables you to redistribute routes learned from various routing information sources into BGP.

Table 254. BGP Neighbor Redistribution Configuration Options

Command Syntax and Usage
[no] `neighbor group` <*group number*> `redistribute default-metric` <*1-4294967294*> Sets default metric of advertised routes. **Command mode:** Router BGP
[no] `neighbor group` <*group number*> `redistribute default-action` {`import`|`originate`|`redistribute`} Sets default route action. Defaults routes can be configured as import, originate, redistribute, or none. **None:** No routes are configured **Import:** Import these routes. **Originate:** The switch sends a default route to peers if it does not have any default routes in its routing table. **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` <*group number*> `redistribute rip` Enables or disables advertising RIP routes. **Command mode:** Router BGP
[no] `neighbor group` <*group number*> `redistribute ospf` Enables or disables advertising OSPF routes. **Command mode:** Router BGP

Table 254. BGP Neighbor Redistribution Configuration Options (continued)

Command Syntax and Usage

[no] `neighbor group` *<group number>* `redistribute fixed`
 	
    Enables or disables advertising fixed routes.
 	
    Command mode: Router BGP

[no] `neighbor group` *<group number>* `redistribute static`
 	
    Enables or disables advertising static routes.
 	
    Command mode: Router BGP

`show ip bgp neighbor group` *<group number>* `redistribute`
 	
    Displays current redistribution configuration.
 	
    Command mode: All except User EXEC

MLD Global Configuration

Table 255 describes the commands used to configure global MLD parameters.

Table 255. MLD Global Configuration Commands

Command Syntax and Usage
`ipv6 mld` Enter MLD global configuration mode. **Command mode:** Global configuration
`default` Resets MLD parameters to their default values. **Command mode:** MLD
`enable` Globally turns MLD on. **Command mode:** MLD
`no enable` Globally turns MLD off. **Command mode:** MLD
exit Exit from MLD configuration mode. **Command mode:** MLD
`show ipv6 mld` Displays the current MLD configuration parameters. **Command mode:** All

MLD Interface Configuration

Table 256 describes the commands used to configure MLD parameters for an interface.

Table 256. MLD Interface Configuration Commands

Command Syntax and Usage
`ipv6 mld default` Resets MLD parameters for the selected interface to their default values. **Command mode:** Interface IP
`[no] ipv6 mld dmrtr enable` Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled. **Command mode:** Interface IP
`ipv6 mld enable` Enables this MLD interface. **Command mode:** Interface IP
`no ipv6 mld enable` Disables this MLD interface. **Command mode:** Interface IP
`[no] ipv6 mld llistnr` *<1-32>* Configures the Last Listener query interval. The default value is 1 second. **Command mode:** Interface IP
`[no] ipv6 mld qintrval` *<2-65535>* Configures the interval for MLD Query Reports. The default value is 125 seconds. **Command mode:** Interface IP
`[no] ipv6 mld qri` *<1000-65535>* Configures the interval for MLD Query Response Reports. The default value is 10,000 milliseconds. **Command mode:** Interface IP
`[no] 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

Table 256. MLD Interface Configuration Commands (continued)

Command Syntax and Usage

`[no] ipv6 mld version <1-2>`
 	
    Defines the MLD protocol version number. The default value is 1.
 	
    Command mode: Interface IP

`show ipv6 mld interface <interface number>`
 	
    Displays the current MLD interface configuration.
 	
    Command mode: All

IGMP Configuration

Table 257 describes the commands used to configure basic IGMP parameters.

Table 257. IGMP Configuration Options

Command Syntax and Usage

`ip igmp enable`
 	
    Globally turns IGMP on.
 	
    Command mode: Global configuration

`no ip igmp enable`
 	
    Globally turns IGMP off.
 	
    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 366
- "IGMP Static Multicast Router Configuration" on page 369
- "IGMP Filtering Configuration" on page 370
- "IGMP Querier Configuration" on page 371

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.

Table 258 describes the commands used to configure IGMP Snooping.

Table 258. IGMP Snooping Configuration Options

Command Syntax and Usage
[no] ip igmp snoop 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 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 query-interval *<1-600>*   Sets the IGMP router query interval, in seconds. The default value is 125.   **Command mode:** Global configuration
[no] ip igmp snoop 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 snoop aggregate   Enables or disables IGMP Membership Report aggregation.   **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 number>*   Adds the selected VLAN(s) to IGMP Snooping.   **Command mode:** Global configuration
no ip igmp snoop vlan *<VLAN number>*   Removes the selected VLAN(s) from IGMP Snooping.   **Command mode:** Global configuration

Table 258.   IGMP Snooping Configuration Options (continued)

Command Syntax and Usage
`no ip igmp snoop vlan all` Removes all VLANs from IGMP Snooping. **Command mode:** Global configuration
`[no] ip igmp snoop vlan <VLAN number> fast-leave` Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove 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 snoop enable` Enables IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop enable` Disables IGMP Snooping. **Command mode:** Global configuration
`[no] ip igmp snoop rtralert` Enables or disables the Router Alert option in IGMP messages. **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

Table 259 describes the commands used to configure IGMP version 3.

Table 259. IGMP Version 3 Configuration Options

Command Syntax and Usage
`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 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
`[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 enable` Enables IGMP version 3. The default value is `disabled`. **Command mode:** Global configuration
`no ip igmp snoop igmpv3 enable` Disables IGMP version 3. **Command mode:** Global configuration
`show ip igmp snoop igmpv3` Displays the current IGMP v3 Snooping configuration. **Command mode:** All except User EXEC

IGMP Static Multicast Router Configuration

Table 260 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 260. IGMP Static Multicast Router Configuration Options

Command Syntax and Usage
`ip igmp mrouter` *\<port alias or number\> \<VLAN number\> \<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 alias or number\> \<VLAN number\> \<version (1-3)\>* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
`no ip igmp mrouter all` Removes all static multicast routers. **Command mode:** Global configuration
`clear ip igmp mrouter` Clears the dynamic multicast router port table. **Command mode:** Global configuration
`show ip igmp mrouter` Displays the current IGMP Multicast Router parameters. **Command mode:** All except User EXEC

IGMP Filtering Configuration

Table 261 describes the commands used to configure an IGMP filter.

Table 261. IGMP Filtering Configuration Options

Command Syntax and Usage
`ip igmp profile` *<1-16>* Configures the IGMP filter. **Command mode:** Global configuration To view command options, see page 370.
`ip igmp filtering` Enables IGMP filtering globally. **Command mode:** Global configuration
`no ip igmp filtering` Disables IGMP filtering globally. **Command mode:** Global configuration
`show ip igmp filtering` Displays the current IGMP Filtering parameters. **Command mode:** All

IGMP Filter Definition

Table 262 describes the commands used to define an IGMP filter.

Table 262. IGMP Filter Definition Options

Command Syntax and Usage
`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
`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
`ip igmp profile` *<1-16>* `enable` Enables this IGMP filter. **Command mode:** Global configuration
`no ip igmp profile` *<1-16>* `enable` Disables this IGMP filter. **Command mode:** Global configuration

Table 262. IGMP Filter Definition Options (continued)

Command Syntax and Usage
`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

Table 263 describes the commands used to configure a port for IGMP filtering.

Table 263. 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
`ip igmp profile <1-16>` Adds an IGMP filter to this port. **Command mode:** Interface port
`no ip igmp profile <1-16>` Removes an IGMP filter from 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 except User EXEC

IGMP Querier Configuration

Table 264 describes the commands used to configure IGMP Querier.

Table 264. IGMP Querier Configuration Options

Command Syntax and Usage
`[no] ip igmp querier vlan <VLAN number or range> enable` Enables or disables IGMP Querier for the selected VLANs. **Command mode:** Global configuration
`[no] ip igmp querier vlan <VLAN number or range> source-ip <IP address>` Configures the IGMP source IP address for the selected VLAN. **Command mode:** Global configuration

Table 264. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
[no] `ip igmp querier vlan` *\<VLAN number or range>* `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 number or range>* `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 number or range>* `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 number or range>* `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 number or range>* `startup-interval` *\<1-608>* Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. **Command mode:** Global configuration
[no] `ip igmp querier vlan` *\<VLAN number or range>* `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 number or range>* `version` `[v1`|`v2`|`v3]` Configures the IGMP version. The default version is `v3`. **Command mode:** Global configuration
[no] `ip igmp querier enable` Enables or disables IGMP Querier. **Command mode:** Global configuration

Table 264. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
show ip igmp querier vlan *<VLAN number or range>* Displays IGMP Querier information for the selected VLAN. **Command mode:** Global configuration
show ip igmp querier Displays the current IGMP Querier parameters. **Command mode:** All

IKEv2 Configuration

Table 265 describes the commands used to configure IKEv2.

Table 265. IKEv2 Options

Command Syntax and Usage
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
[no] ikev2 cookie Enables or disables cookie notification. **Command mode:** Global configuration
show ikev2 Displays the current IKEv2 settings. **Command mode:** All

IKEv2 Proposal Configuration

Table 266 describes the commands used to configure an IKEv2 proposal.

Table 266. 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

Table 266. IKEv2 Proposal Options

Command Syntax and Usage
`integrity {md5|sha1}` Configures the IKEv2 authentication algorithm type. The default value is `sha1`. **Command mode:** IKEv2 proposal
`group {1|2|5|14|24}` Configures the the DH group. The default group is `2`. **Command mode:** IKEv2 proposal

IKEv2 Preshare Key Configuration

Table 267 describes the commands used to configure IKEv2 preshare keys.

Table 267. IKEv2 Preshare Key Options

Command Syntax and Usage
`ikev2 preshare-key local` *<1-32 characters>* Configures the local preshare key. The default value is `ibm123`. **Command mode:** Global configuration
`ikev2 preshare-key remote` *<1-32 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 Identification Configuration

Table 268 describes the commands used to configure IKEv2 identification.

Table 268. 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

Table 268. IKEv2 Identification Options (continued)

Command Syntax and Usage
`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

Table 269 describes the commands used to configure IPsec.

Table 269. IPsec Options

Command Syntax and Usage
`ipsec enable` Enables IPsec. **Command mode:** Global configuration
`no ipsec enable` Disables IPsec. **Command mode:** Global configuration
`show ipsec` Displays the current IPsec settings. **Command mode:** All

IPsec Transform Set Configuration

Table 270 describes the commands used to configure IPsec transforms.

Table 270. IPsec Transform Set Options

Command Syntax and Usage
`ipsec transform-set` *<1-10>* `{ah-md5｜ah-sha1｜esp-3des｜esp-aes-cbc｜esp-des｜esp-md5｜esp-null｜esp｜sha1}` Sets the AH or ESP authentication, encryption, or integrity algorithm. The available algorithms are as follows: – `ah-md5` – `ah-sha1` – `esp-3des` – `esp-aes-cbc` – `esp-des` – `esp-md5` – `esp-null` – `esp-sha1` **Command mode:** Global configuration
`ipsec transform-set` *<1-10>* `transport {ah-md5｜ah-sha1｜esp-3des｜esp-aes-cbc｜esp-des｜esp-md5｜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-md5｜ah-sha1｜esp-3des｜esp-aes-cbc｜esp-des｜esp-md5｜esp-null｜esp｜sha1}` Sets tunnel mode and the AH or ESP authentication, encryption, or integrity algorithm. **Command mode:** Global configuration
`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

Table 271 describes the commands used to configure an IPsec traffic selector.

Table 271. IPsec Traffic Selector Options

Command Syntax and Usage
`ipsec traffic-selector` *<1-10>* `action {permit|deny}` `{any|icmp|tcp} {`*<IPV6 address>*`|any}` Sets the traffic-selector to permit or deny the specified type of traffic. **Command mode:** Global configuration
`src` *<IPv6 address>*`|any` Sets the source IPv6 address. **Command mode:** Global configuration
`ipv6 prefixlen` *<1-128>* Sets the destination IPv6 prefix length. **Command mode:** Global configuration
`dst` *<IPv6 address>*`|any` Sets the destination IP address. **Command mode:** Global configuration
`del` Deletes the traffic selector. **Command mode:** Global configuration
`cur` Displays the current IPsec Traffic Selector settings. **Command mode:** All

IPsec Dynamic Policy Configuration

Table 272 describes the commands used to configure an IPsec dynamic policy.

Table 272. 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
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
sa-lifetime *<120-86400>* Sets the IPsec SA lifetime in seconds. The default value is 86400 seconds. **Command mode:** IPsec dynamic policy
pfs enable|disable Enables/disables perfect forward security. **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

Table 273 describes the commands used to configure an IPsec manual policy.

Table 273. 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 and 16 characters for MD5 encryption.   **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
`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 and 16 characters for MD5 encryption.   **Command mode:** IPsec manual policy
`in-esp cipher-key` *<key code (hexadecimal)>*   Sets the inbound Encapsulating Security Payload (ESP) 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 auth-key` *<key code (hexadecimal)>*   Sets the inbound Encapsulating Security Payload (ESP) authenticator 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

Table 273. IPsec Manual Policy Options (continued)

Command Syntax and Usage
`in-esp auth-key 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 and 16 characters for MD5 encryption. **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 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
`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 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
`out-esp auth-key` *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) authenticator 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 cipher-key` *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) 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 auth-key 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 and 16 characters for MD5 encryption. **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 274. Domain Name Service Options

Command Syntax and Usage
[no] `ip dns primary-server` *<IP address>* [`mgta-port`|`mgtb-port`|`data-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 secondary-server` *<IP address>* [`mgta-port`|`mgtb-port`|`data-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 ipv6 primary-server` *<IP address>* [`mgta-port`|`mgtb-port`|`data-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 secondary-server` *<IP address>* [`mgta-port`|`mgtb-port`|`data-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
`ip dns ipv6 request-version` {`ipv4`|`ipv6`}   Sets the protocol used for the first request to the DNS server, as follows: – IPv4   – IPv6   **Command mode:** Global configuration
[no] `ip dns domain-name` *<string>*   Sets the default domain name used by the switch. For example: `mycompany.com`   **Command mode:** Global configuration
`show ip dns`   Displays the current Domain Name System settings.   **Command mode:** All except User EXEC

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 G8124.

BOOTP relay is turned off by default.

Table 275. Global BOOTP Relay Configuration Options

Command Syntax and Usage

[no] `ip bootp-relay server <`*1-5*`> address <`*IP address*`>`
 	
   Sets the IP address of the selected global BOOTP server.
   Command mode: Global configuration

`ip bootp-relay enable`
 	
   Globally turns on BOOTP relay.
   Command mode: Global configuration

`no ip bootp-relay enable`
 	
   Globally turns off BOOTP relay.
   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 276. BOOTP Relay Broadcast Domain Configuration Options

Command Syntax and Usage
`ip bootp-relay bcast-domain <1-10> vlan <VLAN number>` Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN. **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
`ip bootp-relay bcast-domain <1-10> enable` Enables BOOTP Relay for the broadcast domain. **Command mode:** Global configuration
`no ip bootp-relay bcast-domain <1-10> enable` Disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers. **Command mode:** Global configuration
`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 277. Option 82 Configuration Options

Command Syntax and Usage
`ip bootp-relay information enable` Turns BOOTP Option 82 on. **Command mode:** Global configuration
`[no] ip bootp-relay information enable` Turns BOOTP Option 82 off. **Command mode:** Global configuration
`ip bootp-relay information policy {keep|drop|replace}` Configures the DHCP re-forwarding policy, as follows: – **Keep**: Retains requests that contain relay information if the option 82 information is also present. – **Drop**: Discards requests that contain relay information if the option 82 information is also present. – **Replace**: Replace the relay information in requests that also contain option 82 information. **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 G8124 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. IBM N/OS 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 *IBM N/OS 7.9 Application Guide.*

Table 278. Virtual Router Redundancy Protocol Options

Command Syntax and Usage
`router vrrp` Enter Router VRRP configuration mode. **Command mode:** Global configuration
`holdoff` *<0-255>* Globally sets the time, in seconds, VRRP waits from when the master switch goes down until elevating a new switch to be the master switch. **Command mode:** Router VRRP
`enable` Globally enables VRRP on this switch. **Command mode:** Router VRRP
`no enable` Globally disables VRRP on this switch. **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 279. VRRP Virtual Router Configuration Options

Command Syntax and Usage
`virtual-router` *<1-128>* `virtual-router-id` *<1-255>* 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. 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>* `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
`virtual-router` *<1-128>* `interface` *<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
`virtual-router` *<1-128>* `priority` *<1-254>* Defines the election priority bias for this virtual server. The priority value can be any integer between 1 and 254. The default value is 100. 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. **Command mode:** Router VRRP

Table 279. VRRP Virtual Router Configuration Options (continued)

Command Syntax and Usage
`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
`virtual-router <1-128> timers preempt-delay-time <0-255>` Configures the preempt delay interval. 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. **Command mode:** Router VRRP
[no] `virtual-router <1-128> preemption` 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`. **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 .01 second. 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> enable` Enables this virtual router. **Command mode:** Router VRRP
`no virtual-router <1-128> enable` Disables this virtual router. **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 except User EXEC

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 280. VRRP Priority Tracking Configuration Options

Command Syntax and Usage
[no] `virtual-router` <*1-15*> `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
[no] `virtual-router` <*1-15*> `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` <*1-15*> `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 virtual-router` <*1-15*> `track` Displays the current configuration for priority tracking for this virtual router. **Command mode:** All except User EXEC

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 G8124 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 G8124s in a hot-standby failover configuration, where only one switch is active at any time.

Table 281.   VRRP Virtual Router Group Configuration Options

Command Syntax and Usage
`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 255. 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
`group interface` *<interface number>*   Selects a switch IP interface. The default switch IP interface number is 1.   **Command mode:** Router VRRP
`group priority` *<1-254>*   Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100.   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).   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
`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

Table 281. VRRP Virtual Router Group Configuration Options (continued)

Command Syntax and Usage
[no] group preemption 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). By default, this option is enabled. **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 .01 second. 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
group enable Enables the virtual router group. **Command mode:** Router VRRP
no group enable Disables the virtual router group. **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 except User EXEC

Virtual Router Group Priority Tracking Configuration

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 282.   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 except User EXEC

VRRP Interface Configuration

Note: The *interface* represents the IP interface on which authentication parameters must be configured.

These commands are used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 283. VRRP Interface Options

Command Syntax and Usage
`interface <interface number> authentication {password|none}` Defines the type of authentication that will be used: `none` (no authentication) or `password` (password authentication). **Command mode:** Router VRRP
`[no] interface <interface number> 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 <interface number>` Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted. **Command mode:** Router VRRP
`show ip vrrp interface <interface number>` Displays the current configuration for this IP interface's authentication parameters. **Command mode:** All except User EXEC

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 388), the priority level for the virtual router is increased by a defined amount.

Table 284. VRRP Tracking Configuration Options

Command Syntax and Usage
`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
`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 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
`show ip vrrp tracking-priority-increment`   Displays the current configuration of priority tracking increment values.   **Command mode:** All except User EXEC

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 388) are enabled.

Protocol Independent Multicast Configuration

Table 285. PIM Configuration Options

Command Syntax and Usage
`ip pim component <1-2>` Enter PIM component mode. **Command mode**: Global configuration
`ip pim regstop-ratelimit-period <0-2147483647>` Configures the register stop rate limit, in seconds. The default value is 5. **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
`[no] ip pim pmbr enable` Enables or disables PIM border router. The default setting is `disabled`. **Command mode**: Global configuration
`ip pim enable` Globally turns PIM on. **Command mode**: Global configuration
`no ip pim enable` Globally turns PIM off. **Command mode**: Global configuration
`clear ip pim mroute` Clears PIM multicast router entries. **Command mode**: Global configuration

PIM Component Configuration

Use these commands to configure PIM components.

Table 286. 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 287. RP Candidate Configuration Options

Command Syntax and Usage

`rp-candidate rp-address <group multicast address> <group subnet mask> <IP address>`
 	
    Adds an RP candidate.
 	
    Command mode: PIM Component

`no rp-candidate rp-address <group multicast address> <group subnet mask> <IP address>`
 	
    Removes the specified RP candidate.
 	
    Command mode: PIM Component

`rp-candidate holdtime <0-255>`
 	
    Configures the hold time of the RP candidate, in seconds.
 	
    Command mode: PIM Component

RP Static Configuration

Use these commands to configure a static PIM router Rendezvous Point (RP).

Table 288. 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

Table 289. PIM Interface Configuration Options

Command Syntax and Usage
interface ip *<interface number>* Enter Interface IP mode. **Command mode**: Global Configuration
ip pim hello-interval *<0-65535>* Configures the time interval, in seconds, between PIM Hello packets. The default value is 30. **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. **Command mode**: Interface IP
ip pim cbsr-preference *<0-255>* Configures the candidate bootstrap router preference. **Command mode**: Interface IP
ip pim component-id *<1-2>* Defines the component ID for the interface. **Command mode**: Interface IP
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. **Command mode**: Interface IP

Table 289. PIM Interface Configuration Options (continued)

Command Syntax and Usage
`ip pim dr-priority` *<0-4294967294>* Configures the designated router priority. The default value is 1. **Command mode**: Interface IP
`ip pim override-interval` *<0-65535>* Configures the override interval for the router interface, in 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
`[no] ip pim border-bit` Enables or disables the interface as a border router. The default setting is `disabled`. **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
`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 enable` Enables PIM on the interface. **Command mode**: Interface IP
`no ip pim enable` Disables PIM on the interface. **Command mode**: Interface IP

Table 289. PIM Interface Configuration Options (continued)

Command Syntax and Usage

`show ip pim neighbor-filters`
 	
    Displays the configured PIM neighbor filters.
 	
    Command mode: All

`show ip pim interface [`*`<interface number>`*`|detail|loopback|port` *`<port 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 3: management port A
- Gateway 4: management port B

Table 290 describes the IPv6 Default Gateway Configuration commands.

Table 290. IPv6 Default Gateway Configuration Options

Command Syntax and Usage

`ip gateway6 {1|3|4}  address` *`<IPv6 address>`*
 	
    Configures the IPv6 address of the default gateway, in hexadecimal format
    with colons (such as 3001:0:0:0:0:0:abcd:12).
 	
    Command mode: Global configuration

`[no] ip gateway6 {1|3|4}`
 	
    Enables or disables the default gateway.
 	
    Command mode: Global configuration

`no ip gateway6 {1|3|4}`
 	
    Deletes the default gateway.
 	
    Command mode: Global configuration

`show ipv6 gateway6 {1|3|4}`
 	
    Displays the current IPv6 default gateway configuration.
 	
    Command mode: All

IPv6 Static Route Configuration

Table 291 describes the IPv6 static route configuration commands.

Table 291. IPv6 Static Route Configuration Options

Command Syntax and Usage
`ip route6` *<IPv6 address>* *<prefix length>* *<IPv6 gateway address>* [*<interface number>*] Adds an IPv6 static route. **Command mode**: Global configuration
`no ip route6` *<IPv6 address>* *<prefix length>* Removes the selected route. **Command mode**: Global configuration
`no ip route6` [`destination-address` *<IPv6 address>*| `gateway` *<default gateway address>*|`interface` *<1-128>*|`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

Table 292 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 292. IPv6 Neighbor Discovery Cache Configuration Options

Command Syntax and Usage
`ip neighbors` *<IPv6 address>* *<MAC address>* `vlan` *<VLAN number>* `port` *<port number or alias>* Adds a static entry to the Neighbor Discovery cache table. **Command mode**: Global configuration
`no ip neighbors` {*<IPv6 address>* |`all`} Deletes the selected entry from the static Neighbor Discovery cache table. **Command mode**: Global configuration
`no ip neighbors` [`all if`|`all interface port`|`all vlan` *<VLAN number>*|`all`] 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 293.   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**: All Except User 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 294. IPv6 Neighbor Discovery Prefix Options

Command Syntax and Usage
`interface ip` *<1-124>* Enters Interface IP mode. **Command mode**: Global configuration
`ipv6 nd prefix {`*<IPv6 prefix>* *<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
`no ipv6 nd prefix [`*<IPv6 prefix>* *<prefix length>*`]|interface|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>* *<prefix length>*`}`
  `valid-lifetime` *<0-4294967295>* `[infinite|variable}`
  `prefered-lifetime` *<0-4294967295>* `[infinite|variable}`
 	
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

`ipv6 nd prefix {`*<IPv6 prefix>* *<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

Table 294.   IPv6 Neighbor Discovery Prefix Options (continued)

Command Syntax and Usage
`ipv6 nd prefix {`*`<IPv6 prefix>`* *`<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
`show ipv6 prefix {`*`<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 295.   IPv6 Prefix Policy Table Options

Command Syntax and Usage
`ip prefix-policy` *`<IPv6 prefix>`* *`<prefix length>`* *`<precedence (0-100)>`* *`<label (0-100)>`* Adds a Prefix Policy Table entry. Enter the following parameters: – IPv6 address prefix – Prefix length – **Precedence**: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence. – **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
`no ip prefix-policy` *`<IPv6 prefix>`* *`<prefix length>`* *`<precedence (0-100)>`* *`<label (0-100)>`* Removes a prefix policy table entry. **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 296.   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
`ip address` *<IP address>`* Defines the loopback interface IP address. **Command mode**: Interface loopback
`ip netmask` *<subnet mask>`* Defines the loopback interface subnet mask. **Command mode**: Interface loopback
`ip ospf area` *<area number>`* 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
`enable` Enables the loopback interface. **Command mode**: Interface loopback
`no enable` Disables the loopback 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 297. DHCP Snooping Options

Command Syntax and Usage
`ip dhcp snooping vlan` *<VLAN number>* Adds the selected VLAN to DHCP Snooping. Member ports participate in DHCP Snooping. **Command mode**: Global configuration
`no ip dhcp snooping vlan` *<VLAN number>* Removes the selected VLAN from DHCP Snooping. **Command mode**: Global configuration
`ip dhcp snooping binding` *<MAC address>* `vlan` *<VLAN number>* *<IP address>* `port` *<port alias or number>* `expiry` *<lease>* 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 number>*`]}`
 	
Removes an entry from the binding table.
 	
Command mode: Global configuration

`ip dhcp snooping` Turns on DHCP Snooping. **Command mode**: Global configuration
`no ip dhcp snooping` Turns off DHCP Snooping. **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: – If a DHCP packet from a client contains option 82 information, the information is retained. – When DHCP Snooping forwards a DHCP packet from a client, option 82 information is added to the packet; – When DHCP snooping forward a DHCP packet from a server, option 82 information is removed from the packet. **Command mode**: Global configuration
`show ip dhcp snooping` Displays the current DHCP Snooping parameters. **Command mode**: All

Converged Enhanced Ethernet Configuration

Table 298 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 298. CEE Configuration Options

Command Syntax and Usage
`cee enable` Globally turns CEE on. **Command mode**: Global configuration
`no cee enable` Globally turns CEE off. **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

Table 299 describes the global ETS Priority Group configuration options.

Table 299. Global ETS Priority Group Options

Command Syntax and Usage
`cee global ets priority-group pgid` *<0-7, 15>* `priority` *<802.1p priority (0-7)>* `bandwidth` *<bandwidth percentage (0, 10-100)>*   Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values 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
`[no] cee global ets priority-group pgid` *<0-7, 15>* `description` *<1-31 characters>*   Enter text that describes this Priority Group.   **Command mode**: Global configuration
`cee global ets priority-group pgid` *<0-7, 15>* `priority` *<0-7>*   Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.   **Command mode**: Global configuration
`show cee global ets priority-group` *<0-7, 15>*   Displays the current global ETS Priority Group parameters.   **Command mode**: All
`show cee global ets`   Displays the current global ETS 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.

802.1p PFC Configuration

Table 301 describes the 802.1p Priority Flow Control (PFC) configuration options.

Table 300. PFC 802.1p Configuration Options

Command Syntax and Usage
cee port *<port alias, number, or range>* pfc priority *<0-7>* enable Enables 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
no cee port *<port alias, number, or range>* pfc priority *<0-7>* enable Disables Priority Flow Control on the selected 802.1p priority. **Note**: PFC on 802.1p priority 3 cannot be disabled. **Command mode**: Global configuration
[no] cee port *<port alias, number, or range>* pfc priority *<0-7>* description *<1-31 characters>* Enter text to describe the priority value. **Command mode**: Global configuration
show cee port *<port alias, number, or range>* pfc Displays the current 802.1p Priority Flow Control configuration on the specified port or ports. **Command mode**: All
show cee port *<port alias, number, or range>* pfc priority *<0-7>* Displays the current 802.1p Priority Flow Control parameters. **Command mode**: All

DCBX Port Configuration

Table 301 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 301. Port DCBX Configuration Options

Command Syntax and Usage
`[no] cee port` *\<port alias, number, or range>* `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, number, or range>* `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, number, or range>* `dcbx ets advertiFse` 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, number, or range>* `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, number, or range>* `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, number, or range>* `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
`no cee port` *\<port alias, number, or range>* `dcbx enable` Disables DCBX on the port. **Command mode**: Global configuration
`cee port` *\<port alias, number, or range>* `dcbx enable` Enables DCBX on the port. **Command mode**: Global configuration
`show cee port` *\<port alias, number, or range>* `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.

Table 302 describes the FCoE configuration options.

Table 302. FCoE Configuration Options

Command Syntax and Usage
`fcoe fips enable` Globally turns FIP Snooping on. **Command mode**: Global configuration
`no fcoe fips enable` Globally turns FIP Snooping off. **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
`[no] fcoe fips automatic-vlan` Enables or disables automatic VLAN creation, based on response received from the connected device. **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.

Table 303 describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 303. Port FIP Snooping Options

Command Syntax and Usage
fcoe fips port <*port alias or number*> fcf-mode [auto|on|off] Configures FCoE Forwarding (FCF) on the port, as follows: – on: Configures the port as a Fibre Channel Forwarding (FCF) port. – off: Configures the port as an FCoE node (ENode port). – auto: Automatically detect the configuration of the connected device, and configure this port to match. **Command mode**: Global configuration
fcoe fips port <*port alias or number*> enable Enables FIP Snooping on the port. The default setting is enabled. **Command mode**: Global configuration
no fcoe fips port <*port alias or number*> enable Disables FIP Snooping on the port. **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 1757.

The following sections describe the Remote Monitoring (RMON) configuration options.

RMON History Configuration

Table 304 describes the RMON History commands.

Table 304. 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>* 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
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>* 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>*   Deletes the selected History index.   **Command mode**: Global configuration
show rmon history   Displays the current RMON History parameters.   **Command mode**: All

RMON Event Configuration

Table 305 describes the RMON Event commands.

Table 305. 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>* `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
`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>* 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.

Table 306 describes the RMON alarm commands.

Table 306. RMON Alarm Configuration Options

Command Syntax and Usage
`rmon alarm` *<1-65535>* `oid` *<1-127 characters>*   Configures an alarm MIB Object Identifier.   **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>* `sample abs|delta`   Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: – `abs`—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval.   – `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
`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>* `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>* `falling-limit` *<-2147483647 - 214748364)*   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

Table 306. RMON Alarm Configuration Options (continued)

Command Syntax and Usage
`rmon alarm <1-65535> rising-crossing-index <1-65535>` Configures the rising alarm event index that is triggered when a rising threshold is crossed. **Command mode**: Global configuration
`rmon alarm <1-65535> falling-crossing-index <1-65535>` Configures the falling alarm event index that is triggered when a falling threshold is crossed. **Command mode**: Global configuration
`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>` Deletes the selected RMON Alarm index. **Command mode**: Global configuration
`show rmon alarm` Displays the current RMON Alarm parameters. **Command mode**: All

Virtualization Configuration

Table 307 describes the virtualization configuration options.

Table 307. Virtualization Configuration Options

Command Syntax and Usage
`virt enable` Enables VMready. Before you enable VMready, you must define one or more server ports. See "Server Port Configuration" on page 246. **Command mode**: Global configuration
`no virt enable` Disables VMready. **Note**: 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

Table 308 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 308. VM Bandwidth Management Options

Command Syntax and Usage

`virt vmpolicy vmbwidth [<MAC address>|<UUID>|<name>|`
`    <IP address>|<index number>] txrate <64-10000>`
`    <max. burst (32-4096)> <ACL number>`
 	
The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in megabits 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: 32, 64, 128, 256, 512, 1024, 2048, 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>] bwctrl`
 	
Enables or disables bandwidth control on the VM policy.
 	
Command mode: Global configuration

Table 308. VM Bandwidth Management Options (continued)

Command Syntax and Usage
`[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 vmbandwidth [<`*MAC address*`>|<`*UUID*`>|<`*name*`>| <`*IP address*`>|<`*index number*`>]` Displays the current VM bandwidth management parameters. **Command mode:** All

Virtual NIC Configuration

Table 309 describes the Virtual NIC (vNIC) configuration options.

Table 309. Virtual NIC Options

Command Syntax and Usage
`vnic enable` Globally turns vNIC on. **Command mode**: Global configuration
`no vnic enable` Globally turns vNIC off. **Command mode**: Global configuration
`show vnic` Displays the current vNIC parameters. **Command mode**: Global configuration

vNIC Port Configuration

Table 310 describes the Virtual NIC (vNIC) port configuration options.

Table 310. vNIC Port Configuration Options

Command Syntax and Usage
`vnic port` *<port alias or number>* `index` *<1-4>* Enters vNIC Configuration mode. **Note**: This command is valid for internal server ports only. **Command mode**: Global configuration
`bandwidth` *<1-100>* Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example: – 1 = 100 Mbps – 10 = 1000 Mbps **Command mode**: vNIC configuration
`enable` Enables the vNIC. **Command mode**: vNIC configuration
`no enable` Disables the vNIC. **Command mode**: vNIC configuration

Virtual NIC Group Configuration

Table 311 describes the Virtual NIC (vNIC) Group configuration options.

Table 311. vNIC Group Configuration Options

Command Syntax and Usage
`vnic vnicgroup` *<1-32>* Enters vNIC Group Configuration mode. **Command mode:** Global Configuration
`vlan` *<VLAN number>* Assigns a VLAN to the vNIC Group. **Command mode:** vNIC Group configuration
`[no] failover` Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable only the affected vNIC links on the port. Other port functions continue to operate normally. The default setting is `disabled`. **Command mode:** vNIC Group configuration

Table 311. vNIC Group Configuration Options (continued)

Command Syntax and Usage
`member` *<vNIC number>* Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: `1.1` **Command mode:** vNIC Group configuration
`no member` *<vNIC number>* Removes the selected vNIC from the vNIC Group. **Command mode:** vNIC Group configuration
`port` *<port number or alias>* Adds the selected switch port to the vNIC Group. **Command mode:** vNIC Group configuration
`no port` *<port number or alias>* Removes the selected switch port from the vNIC Group. **Command mode:** vNIC Group configuration
`trunk` *<trunk number>* Adds the selected trunk group to the vNIC Group. **Command mode:** vNIC Group configuration
`no trunk` *<trunk number>* Removes the selected trunk group from the vNIC Group. **Command mode:** vNIC Group configuration
`key` *<trunk number>* Adds the uplink LACP trunk to the vNIC Group. **Command mode:** vNIC Group configuration
`no key` *<trunk number>* Removes the selected uplink LACP trunk from the vNIC Group. **Command mode:** vNIC Group configuration
`enable` Enables the vNIC Group. **Command mode:** vNIC Group configuration
`no enable` Disables the vNIC Group. **Command mode:** vNIC Group configuration

Table 311. vNIC Group Configuration Options (continued)

Command Syntax and Usage
`no vnic vnicgroup` *<1-32>* Deletes the selected vNIC Group. **Command mode:** Global configuration
`show vnicgroup` Displays the current vNIC Group parameters. **Command mode:** All

VM Group Configuration

Table 312 describes the VM group configuration options.A VM group is a collection of members, such as VMs, ports, or trunk groups. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 312. VM Group Configuration Options

Command Syntax and Usage
`virt vmgroup` *<1-4096>* `vlan` *<VLAN number>* 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>* `vmap` *<VMAP number>* `serverports|non-serverports` Assigns the selected VLAN Map to 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 271. **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>* `vm` [*<MAC address>|<UUID>|<name>|<IP address>|* *<index number>*] Adds a VM to 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
`no virt vmgroup` *<1-4096>* `vm` [*<MAC address>|<UUID>|<name>|* *<IP address>|<index number>*] Removes a VM 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`). **Command mode:** Global configuration

Table 312. VM Group Configuration Options (continued)

Command Syntax and Usage
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
virt vmgroup *<1-4096>* port *<port alias or number>* Adds the selected port to 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>* port *<port alias or number>* Removes the selected port from the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* portchannel *<trunk number>* Adds the selected trunk group to the VM group. **Command mode:** Global configuration
no virt vmgroup *<1-4096>* portchannel *<trunk number>* Removes the selected trunk group from the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* key *<1-65535>* Adds an LACP *admin key* to the VM group. LACP trunks formed with this *admin key* will be included in the VM group. **Command mode:** Global configuration
no virt vmgroup *<1-4096>* key *<1-65535>* Removes an LACP *admin key* from the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* stg *<STG number>* Assigns the VM group to a Spanning Tree Group (STG). **Command mode:** Global configuration

Table 312. VM Group Configuration Options (continued)

Command Syntax and Usage

`virt vmgroup <1-4096> validate [basic|advanced]`
 	
Enables MAC address spoof prevention for the specified VM group. Default setting is disabled.
 	
  – `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.
 	
  – `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.
 	
Command mode: Global configuration

`no virt vmgroup <1-4096> validate` Disables MAC address spoof prevention for the specified 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

Table 313 describes the VM Check validation options used for MAC address spoof prevention.

Table 313. VM Check Configuration Options

Command Syntax and Usage
`virt vmcheck acls max <1-127>`   Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50.   **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 basic {link｜log}`   Sets up action taken when detecting MAC address spoofing in basic validation mode: – `link` registers a syslog entry and disables the corresponding switch port   – `log` registers a syslog entry   Default setting is `link`.   **Command mode:** Global configuration
`virt vmcheck action advanced {acl｜link｜log}`   Sets up action taken when detecting MAC address spoofing in advanced validation mode: – `acl` registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address   – `link` registers a syslog entry and disables the corresponding switch port   – `log` registers a syslog entry   Default setting is `acl`.   **Command mode:** Global configuration
`[no] virt vmcheck trust <ports>`   Enables or disables trusted ports for VM communication. By default, all ports are disabled.   **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

Table 313. VM Check Configuration Options

Command Syntax and Usage
`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
`show virt vmcheck` Displays the current VM Check settings. See for sample output. **Command mode**: Global configuration

VM Profile Configuration

Table 314 describes the VM Profiles configuration options.

Table 314. 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 32 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)>* `vlan` *<VLAN number>* Assigns a VLAN to the VM profile. **Command mode:** Global configuration

`[no] 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:
– Average traffic, in Kilobits per second
– Maximum burst size, in Kilobytes
– Peak traffic, in Kilobits per second
– Delete traffic shaping parameters.
Command mode: Global configuration

`[no] 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:
– Average traffic, in Kilobits per second
– Maximum burst size, in Kilobytes
– Peak traffic, in Kilobits per second
– Delete traffic shaping parameters.
Command mode: Global configuration

`show virt vmprofile` `[`*<profile name>*`]` Displays the current VM Profile parameters. **Command mode:** All

VMWare Configuration

Table 315 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 315. 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
`[no] 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: – IP address of the Virtual Center   – User name and password for the Virtual Center   – Whether to authenticate the SSL security certificate (yes or no)   **Command mode:** Global configuration
`virt vmware hello [enable|haddr `*<IP_address>*`|hport `*<port_no>*`|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.   – `enable` enables CDP advertisements transmission.   – `haddr` advertises a specific IP address instead of the default 0.0.0.0 IP.   – `hport` enables ports on which CDP advertisements are sent.   – `htimer` sets the number of seconds between successive CDP advertisements. Default value is 30.   **Command mode:** Global configuration
`no virt vmware hello [enable|hport `*<port_no>*`]`   Disables CDP advertisement transmissions completely or only on specific ports.   **Command mode**: Global configuration
`default virt vmware hbport`   Sets to default esx/esxi server to vcenter heartbeat udp port.   **Command mode**: Global configuration
`default virt vmware hello htimer`   Sets to default HELLO periodicity.   **Command mode**: Global configuration

Table 315. VM Ware Configuration Options

Command Syntax and Usage

`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 IBM N/OS CLI and the Miscellaneous VMready Configuration Menu. Table 315 describes the VMready configuration options.

Table 316. VMready Configuration Options

Command Syntax and Usage
`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:** Global configuration
`virt vmrmisc lmac` Enables the switch to treat locally administered MAC addresses as VMs. **Command mode:** Global configuration
`no virt vmrmisc lmac` Disables the switch from treating locally administered MAC addresses as VMs. **Command mode:** Global configuration

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 317. Microburst Detection Configuration Options

Command Syntax and Usage
`[no] microburst enable` Enables or disables microburst detection. Default setting is disabled. **Command mode:** Global configuration
`microburst interval <2-10000>` Configures microburst detection interval granularity in milliseconds. Default setting is 5. **Command mode:** Global configuration
`microburst port-threshold <port no.> <1-42650>` 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. Default value is 42650. **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
`clear microburst counters` Resets microburst packet counters. **Command mode:** Privileged EXEC

Configuration Dump

The dump program writes the current switch configuration to the terminal screen. To start the dump program, at the prompt, enter:

```
G8124(config)# 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 .

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp|sftp}` 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:

```
Router(config)# copy running-config ftp

    or

Router(config)# copy running-config tftp

    or

Router(config)# copy running-config sftp
```

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 {ftp|tftp|sftp} 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:

```
Router(config)# copy ftp running-config

    or

Router(config)# copy tftp running-config

    or

Router(config)# copy sftp running-config
```

The switch prompts you for the server address and filename.

-
-

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 reset, the port returns to its normally configured operation.

These commands enable you to alter switch operational characteristics without affecting switch configuration.

Table 318. General Operations Commands

Command Syntax and Usage
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
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
clear logging Clears all Syslog messages. **Command Mode**: Privileged EXEC
ntp send Allows the user to send requests to the NTP server. **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 319. Port Operations

Command Syntax and Usage
[no] interface port *<port number or alias>* rmon   Temporarily enables or disables remote monitoring of the port. The port will be returned to its configured operation mode when the switch is reset.   **Command Mode**: Privileged EXEC
no interface port *<port number or alias>* shutdown   Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.   **Command Mode**: Privileged EXEC
interface port *<port number or alias>* shutdown   Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.   **Command Mode**: Privileged EXEC
interface port *<port number or alias>* learning   Temporarily enables FDB learning on the port.   **Command Mode**: Privileged EXEC
no interface port *<port number or alias>* learning   Temporarily disables FDB learning on the port.   **Command Mode**: Privileged EXEC
show interface port *<port number or alias>* operation   Displays the port interface operational state.   **Command Mode**: Privileged EXEC

Operations-Level FCoE Commands

Fiber Channel over Ethernet (FCoE) operations commands are listed in the following table.

Table 320. FCoE Operations

Command Syntax and Usage
`no fcoe fips fcf` *\<FCF MAC address>* [*\<vlan number>*] Deletes the selected FCoE Forwarder (FCF) and any associated ACLs. **Command Mode**: Privileged EXEC

Operations-Level VRRP Commands

Operations-level VRRP commands are listed in the following table.

Table 321. Virtual Router Redundancy Operations

Command Syntax and Usage
`router vrrp backup {`*<virtual router number (1-15)>*`|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:
– This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same)
– This switch's virtual router has a higher priority and preemption is enabled.
– There are no other virtual routers available to take master control.
Command Mode: Privileged EXEC

Operations-Level BGP Commands

Table 322. IP BGP Operations

Command Syntax and Usage

`router bgp start` *\<peer number\>*
 	
    Starts the peer session.
 	
    Command Mode: Privileged EXEC

`router bgp stop` *\<peer number\>*
 	
    Stops the peer session.
 	
    Command Mode: Privileged EXEC

`show ip bgp state`
 	
    Displays the current BGP operational state.
 	
    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 323. VMware Operations

Command Syntax and Usage
`virt vmware pg` [*\<Port Group name\> \<host ID\> \<VSwitch name\> \<VLAN number\> \<shaping-enabled\> \<average-Kbps\> \<burst-KB\> \<peak-Kbps\>*] Adds a Port Group to a VMware host. You are prompted for the following information: – Port Group name – VMware host ID (Use host UUID, host IP address, or host name.) – Virtual Switch name – VLAN ID of the Port Group – 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
`virt vmware vsw` *\<host ID\> \<Virtual Switch name\>* Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host: – UUID – IP address – Host name **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: – UUID – IP address – Host name **Command Mode**: All
`no virt vmware vsw` *\<host ID\> \<Virtual Switch name\>* Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host: – UUID – IP address – Host name **Command Mode**: All

Table 323. VMware Operations (continued)

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:
  – UUID
  – IP address
  – 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 scan` Performs a scan of the VM Agent, and updates VM information. **Command Mode**: All
`virt vmware vmacpg` *\<MAC address\> \<Port Group name\>* Changes a VM NIC's configured Port Group. **Command Mode**: All

`virt vmware updpg` *\<Port Group name\> \<host ID\> \<VLAN number\>* *[\<shaping enabled\> \<average (1-1000000)\> \<burst (1-1000000)\> \<peak (1-1000000)\>]*
 	
Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID:
  – UUID
  – IP address
  – Host name
 	
Enter the traffic shaping parameters as follows:
  – Shaping enabled
  – Average traffic, in Kilobits per second
  – Maximum burst size, in Kilobytes
  – Peak traffic, in Kilobits per second
 	
Delete traffic shaping parameters.
 	
Command Mode: All

VMware Distributed Virtual Switch Operations

Use these commands to administer a VMware Distributed Virtual Switch (dvSwitch).

Table 324. 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 del` *<datacenter name> <dvSwitch name>* Removes the specified dvSwitch from the specified DataCenter. **Command Mode**: All

`virt vmware dvswitch addhost` *<dvSwitch name>*
  <host UUID|IP address|host name>
 	
Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host:
  – UUID
  – IP address
  – Host name
 	
Command Mode: All

`virt vmware dvswitch remhost`
  <dvSwitch name> <host UUID|IP address|host name>
 	
Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host:
  – UUID
  – IP address
  – Host name
 	
Command Mode: All

`virt vmware dvswitch addUplink` *<dvSwitch name> <host ID> <uplink name>* Adds the specified physical NIC to the specified dvSwitch uplink ports. **Command Mode**: All
`virt vmware dvswitch remUplink` *<dvSwitch name> <host ID> <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 325. VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)

Command Syntax and Usage

virt vmware dpg add *<port group name> <dvSwitch name> <VLAN ID>*
  [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:
 	
– ishaping: Enables ingress shaping. Supply the following information:
  • average bandwidth in KB per second
  • burst size in KB
  • peak bandwidth in KB per second
– eshaping: Enables egress shaping. Supply the following information:
  • average bandwidth in KB per second
  • burst size in KB
  • peak bandwidth in KB 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

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:
 	
– ishaping: Enables ingress shaping. Supply the following information:
  • average bandwidth in KB per second
  • burst size in KB
  • peak bandwidth in KB per second
– eshaping: Enables egress shaping. Supply the following information:
  • average bandwidth in KB per second
  • burst size in KB
  • peak bandwidth in KB 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

Edge Virtual Bridge Operations

Edge Virtual Bridge operations commands are listed in the following table:

Table 326. 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 vsidb [mgrid <0-255> | typeid <1-16777215> | version <0-255>]` Clears local VSI types cache. **Command mode**: Privileged EXEC
`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

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 is next reset
- Selecting a configuration block to be used when the switch is next reset
- 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" in the *Command Reference*.

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 327. Scheduled Reboot Options

Command Syntax and Usage

`boot schedule` *\<day\>* *\<time (hh:mm)\>*
 	
 Configures the switch reset time. The following options are valid for the `day` value:
 	
 `monday`
 `tuesday`
 `wednesday`
 `thursday`
 `friday`
 `saturday`
 `sunday`
 	
 Command Mode: Global configuration

`no boot schedule`   Cancels the switch reset time.   **Command Mode**: Global configuration
`show boot`   Displays the current switch reboot schedule.   **Command Mode**: All except User EXEC

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 328. Netboot Options

Command Syntax and Usage
`boot netboot enable` Enables 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 enable` Disables Netboot. **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
`[no] boot netboot cfgfile` *‹1-31 characters›* Defines the file path for the configuration file on the TFTP server. For example: `/directory/sub/config.cfg` **Command Mode**: Global configuration
`show boot` Displays the current Netboot parameters. **Command Mode**: All

•

Updating the Switch Software Image

The switch software image is the executable code running on the RackSwitch G8124. 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.

Click on software updates. Use the following command to determine the current software version: `show boot`

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 reset

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:

```
Router# copy {ftp|tftp|sftp} {image1│image2│boot-image}
```

2. Select a port to use for downloading the image

```
Port type [DATA|MGTB|MGTA]:
```

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:

```
Router(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 reset:

```
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:

```
Router# copy {image1│image2│boot-image} {ftp|tftp|sftp}
```

2. Select a port type to use for uploading the image.

```
Port type [DATA|MGTB|MGTA]:
```

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 G8124, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform a save operation (`copy running-config startup-config`), 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 G8124 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 G8124 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 reset:

```
Router (config)# boot configuration-block {active│backup│factory}
```

Resetting the Switch

You can reset the switch to make your software image file and configuration block changes occur.

Note: Resetting 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 reset (reload) the switch:

```
>> Router# reload
```

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) ?
```

Changing the Switch Profile

The IBM N/OS software for the G8124 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 IBM N/OS 7.9 *Application Guide*.

To change the deployment profile, select the new profile and reset the G8124. Use the following command to select a new profile:

```
Router(config)# boot profile {default | acl | ipmc-opt}
```

```
Router(config)# boot profile {default|routing|aggreg|access|iptv|hft}
```

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.

```
Resetting the System ...
Memory Test ...............................

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Boot in recovery mode
4 - Xmodem download (for boot image only - use recovery mode for application
images)
5 - Reboot
6 - Exit

Please choose your menu option: 1
Current boot image is 1. Enter image to boot: 1 or 2: 2
Booting from image 2
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2 and follow the screen prompts.
- To boot in recovery mode and to restore the application image, press 3 and follow the screen prompts.
- To download the boot image via xmodem, press 4 and follow the screen prompts.
- To reboot the system, press 5 and follow the screen prompts.
- To exit the Boot Management menu, press 6. The booting process continues.

Recovering from a Failed Upgrade

Use the following procedure to recover from a failed software 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, CRT, 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. Select **3** for **Xmodem download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

5. 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.

6. Select the Boot Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash............. done

Writing to Flash............done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash.............................................. done

Writing to Flash...............................................done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash........... done

Writing to Flash...........done

Protected 8 sectors
```

7. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

8. Press the Escape key (<**Esc**>) to re-display the Boot Management menu.

9. Select **3** to start a new **XModem Download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
## Switch baudrate to 115200 bps and press ENTER ...
```

10. Press <**Enter**> to continue the download.

11. Select the OS Image to download. The XModem initiates the file transfer. When the download is complete, a message similar to the following is displayed:

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** Switch OS ****


Please choose the Switch OS Image to upgrade [1|2|n] :
```

12. Select the image number to load the new image (1 or 2). It is recommended that you select 1. A message similar to the following is displayed:

```
Switch OS Image 1 ...

Un-Protected 27 sectors

Erasing Flash.............................. done

Writing to Flash.............................done

Protected 27 sectors
```

13. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
## Switch baudrate to 9600 bps and press ESC ...
```

14. Press the Escape key (<**Esc>**) to re-display the Boot Management menu.

Select **4** to exit and boot the new image.

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 G8124 after any one of the following occurs:

- The watchdog timer forces a switch reset. 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 329. General Maintenance Commands

Command Syntax and Usage
`show flash-dump-uuencode` Displays dump information in uuencoded format. For details, see . **Command mode:** All
`copy flash-dump {tftp|ftp|sftp} {data|mgta|mgtb}` Saves the system dump information via TFTP, FTP or SFTP. For details, see . **Command mode:** Privileged EXEC
`copy <switch filename> tftp address <TFTP server address> filename <filename on TFTP server>` Saves a file via TFTP.sC **Command mode:** Privileged EXEC
`clear flash-dump` Clears dump information from flash memory. **Command mode:** Privileged EXEC
`copy log tftp {data|mgta|mgtb}` Saves the system log file (SYSLOG) via TFTP. **Command mode:** Privileged EXEC
`clear log` Clears the system log file (SYSLOG). **Command mode:** Privileged EXEC

Table 329. General Maintenance Commands (continued)

Command Syntax and Usage
`show tech-support [l2|l3|link|port]` Dumps all G8124 information, statistics, and configuration. You can log the output (`tsdmp`) into a file. To filter the information, use the following options: – `l2` displays only Layer 2-related information – `l3` displays only Layer 3-related information – `link` displays only link status-related information – `port` displays only port-related information **Command mode:** All except User EXEC
`copy tech-support tftp {data|mgta|mgtb}` Redirects the technical support dump (tsdmp) to an external TFTP server. **Command mode:** Privileged EXEC
`copy tech-support ftp {data|mgta|mgtb}` Redirects the technical support dump (tsdmp) to an external FTP server. **Command mode:** Privileged EXEC
`copy tech-support sftp {data|mgt}` Redirects the technical support dump (tsdmp) to an external SFTP server. **Command mode:** Privileged 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 330. 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: – `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) – `xxxxxxxxxxxx` (such as `080020123456`) **Command mode:** All
`show mac-address-table interface port` <*port number or alias*> Displays all FDB entries for a particular port. **Command mode:** All
`show mac-address-table vlan` <*VLAN number*> Displays all FDB entries on a single VLAN. **Command mode:** All
`show mac-address-table multicast` Displays all Multicast MAC entries in the FDB. **Command mode:** All
`show mac-address-table static` Displays static entries in the FBD. **Command mode:** All except User EXEC
`no mac-address-table` {`static`|`multicast`} {`all`|<*MAC address*> <*VLAN number*>} 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 reset occurs

If the switch resets 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 331. 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 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

`debug dumpbt` Displays the backtrace log. **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 reset occurred. **Command mode:** Privileged EXEC
`clear flash-config` Deletes all flash configuration blocks. **Command mode:** Privileged EXEC
`[no] debug pregs` *<port>* `[`*<device offset>* `[`*<value>*`]]` AEL Physical Register Set/Get/Dump for the selected port. This option is reserved for technical support use only. **Command mode:** Privileged EXEC
`[no] debug sreg` *<register>* `[`*<hexadecimal value>*`]` Bali Switch Register Set/Get. This option is reserved for technical support use only. **Command mode:** Privileged EXEC
`debug pstat` *<port alias or number>* Displays all port statistics for the selected port. **Command mode:** Privileged EXEC

Table 331. Miscellaneous Debug Options

Command Syntax and Usage
[no] debug lacp packet [receive|transmit|both] [port *<port numbers>*] Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP. The following parameters are available: – receive filters only LACP packets received – transmit filters only LACP packets sent – both filters LACP packets either sent or received – port filters LACP packets sent/received on specific ports By default, LACP debugging is disabled. **Command mode:** Privileged EXEC
[no] debug spanning-tree bpdu [receive|transmit] Enables/disables debugging for Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames sent or received. The following parameters are available: – receive filters only BPDU frames received – transmit filters only BPDU frames sent By default, STP BPDU debugging is disabled. **Command mode**: Privileged EXEC

IPsec Debugging

Tabxlx describes the IPsec debugging commands.

Table 332. 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 ipsec` Enables or disables all IPsec debug messages. **Command mode:** Privileged EXEC
`[no] debug sec info` Displays the current security debug flag. **Command mode:** Privileged EXEC

DCBX Maintenance

Table 333 describes the DCBX maintenance commands.

Table 333. 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>* `ets` Displays DCBX ETS state-machine information. **Command mode:** All
`show cee information dcbx port` *<port alias or number>* `pfc` Displays DCBX PFC 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>* `feature` Displays information about the Feature state machine for the selected port. **Command mode:** All
`show dcbx transmit` Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV for the selected port. **Command mode:** All
`show dcbx receive` Displays the Type-Length-Value (TLV) list received in the DCBX TLV for the selected port. **Command mode:** All

LLDP Cache Manipulation

Table 334 describes the LLDP cache manipulation commands.

Table 334. LLDP Cache Manipulation Options

Command Syntax and Usage
show lldp port *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information. **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**]** Displays information received from LLDP -capable devices. For more information, see page 37. **Command mode:** All
show lldp Displays all LLDP information. **Command mode:** All
clear lldp Clears the LLDP cache. **Command mode:** Privileged EXEC

ARP Cache Maintenance

Table 335 describes the ARP cache maintenance commands.

Table 335. Address Resolution Protocol Maintenance Options

Command Syntax and Usage
`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 vlan` *‹VLAN number›* Shows ARP entries on a single VLAN. **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` Shows all ARP entries. **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 .

IP Route Manipulation

Table 336 describes the IP route manipulation commands.

Table 336. IP Route Manipulation Options

Command Syntax and Usage
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 type {indirect|direct|local|broadcast| martian|multicast} Shows routes of a single type. For a description of IP routing types, see Table 36 on page 53 **Command mode:** All
show ip route tag {fixed|static|address|rip|ospf|broadcast| martian|multicast} Shows routes of a single tag. For a description of IP routing tags, see Table 37 on page 53 **Command mode:** All
show ip route interface *<IP interface>* Shows routes on a single interface. **Command mode:** All
show ip route Shows all routes. **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 52.

IGMP Snooping Maintenance

Table 337 describes the IGMP Snooping maintenance commands.

Table 337. IGMP Multicast Group Maintenance Options

Command Syntax and Usage
`show ip igmp groups address` *\<IP address\>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
`show ip igmp groups vlan` *\<VLAN number\>* Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
`show ip igmp groups interface port` *\<port number or alias\>* Displays all IGMP multicast groups on selected ports. **Command mode:** All
`show ip igmp groups portchannel` *\<trunk number\>* Displays all IGMP multicast groups on a single trunk group. **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` Displays information for all multicast groups. **Command mode:** All
`clear ip igmp groups` Clears the IGMP group table. **Command mode:** Privileged EXEC

IGMP Multicast Routers Maintenance

Table 338 describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 338. IGMP Multicast Router Maintenance Commands

Command Syntax and Usage
`show ip igmp mrouter vlan` *‹VLAN number›* Displays IGMP Mrouter information for a single VLAN. **Command mode:** All
`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 snoop igmpv3` Displays IGMPv3 snooping information. **Command mode:** All
`show ip igmp relay` Displays IGMP relay information. **Command mode:** All
`show ip igmp querier vlan` *‹VLAN number›* Displays IGMP querier information for a single VLAN. **Command mode:** All
`clear ip igmp mrouter` Clears the dynamic IGMP Mrouter port table. **Command mode:** Privileged EXEC

MLD Multicast Group Maintenance

Table 339 describes the maintenance commands for MLD multicast group maintenance.

Table 339. MLD Multicast Group Maintenance Commands

Command Syntax and Usage
`groups` Displays all MLD groups. **Command mode:** All
`find` *\<IPv6 address>* Shows a single MLD group by its IP address. **Command mode:** All
`vlan` *\<VLAN number>* Shows all MLD groups on a single VLAN. **Command mode:** All
`port` *\<port alias or number>* Shows all MLD groups on a single port. **Command mode:** All
`trunk` *\<trunk number>* Displays all MLD groups on a single trunk group. **Command mode:** All
`if` *\<interface number>* Shows MLD interface information. **Command mode:** All
`mrclear` Clears dynamic MLD multicast router group tables from switch memory. **Command mode:** All
`grclear` Clears dynamic MLD registered group tables from switch memory. **Command mode:** All
`clear` Clears dynamic MLD group tables from switch memory. **Command mode:** All
`show ip igmp mrouter vlan` *\<VLAN number>* Displays IGMP Mrouter information for a single VLAN. **Command mode:** All

Table 339. MLD Multicast Group Maintenance Commands

Command Syntax and Usage
`show ip igmp mrouter` Displays information for all Mrouters. **Command mode:** All
`clear ip igmp mrouter` Clears the IGMP Mrouter port table. **Command mode:** Privileged EXEC

IPv6 Neighbor Cache Manipulation

Table 340 describes the IPv6 Neighbor Cache manipulation commands.

Table 340. IPv6 Neighbor Cache Manipulation Options

Command Syntax and Usage
`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 number or alias>* Shows IPv6 Neighbor Cache entries on a single port. **Command mode:** All
`show ipv6 neighbors vlan` *<VLAN number>* Shows IPv6 Neighbor Cache entries on a single VLAN. **Command mode:** All
`show ipv6 neighbors static` Shows static IPv6 Neighbor Cache entries. **Command mode:** All
`show ipv6 neighbors` Shows all IPv6 Neighbor Cache entries. **Command mode:** All
`show ipv6 neighbors counters` Displays IPv6 Neighbor Cache statistics. **Command mode**: All
`clear ipv6 neighbors` Clears all IPv6 Neighbor Cache entries from switch memory. **Command mode:** Privileged EXEC
`clear ipv6 neighbors counters` Clears all IPv6 Neighbor Cache statistics from switch memory. **Command mode**: Privileged EXEC

IPv6 Route Maintenance

Table 341 describes the IPv6 route maintenance commands.

Table 341. IPv6 Route Maintenance Options

Command Syntax and Usage
`show ipv6 route address` *<IPv6 address>* Show a single route by destination IP address. **Command mode:** All
`show ipv6 route gateway` *<IPv6 gateway number>* Show routes to a single gateway. **Command mode:** All
`show ipv6 route interface` *<interface number>* Show routes on a single IP interface. **Command mode:** All
`show ipv6 route type {connected|static|ospf}` Show routes of a single type. **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` Shows all IPv6 routes. **Command mode:** All
`clear ipv6 route` Clears all IPv6 routes. **Command mode:** Privileged EXEC

Uuencode Flash Dump

Using this command, dump information is presented in uuencoded format. This format makes it easy to capture the dump information as a file or a string of characters.

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `show flash-dump-uuencode` command. This will ensure that you do not lose any information. Once entered, the `show flash-dump-uuencode` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `show flash-dump-uuencode` command, dump information can be read multiple times. The command does not cause the information to be updated or cleared from flash memory.

Note: Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see page 473.

To access dump information, enter:

```
Router# show flash-dump-uuencode
```

The dump information is displayed on your screen and, if you have configured your communication software to do so, captured to a file. If the dump region is empty, the following appears:

```
No FLASH dump available.
```

TFTP, SFTP or FTP System Dump Put

Use these commands to `put` (save) the system dump to a TFTP or FTP server.

Note: If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump tftp`), 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:

```
Router# 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:

```
Router# 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:

```
Router# 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:

```
Router# 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. IBM N/OS System Log Messages

The RackSwitch G8124 (G8124) uses the following syntax when outputting system log (syslog) messages:

*<Time stamp><IP/Hostname><Log Label>*IBMOS*<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!
AMP	Access port *<port>* is receiving AMP packets from aggregator switch *<MAC address>*
AMP	Access trunk *<trunk ID>* is receiving AMP packets from {access | aggregator} switch *<MAC address>*
AMP	Aggregator {port *<port>* | trunk *<trunk ID>*} is receiving AMP packets from access switch *<MAC address>*
AMP	AMP group <group> topology is DOWN
AMP	AMP keep-alive timeout on {port *<port>* | trunk *<trunk ID>*}
AMP	AMP packets looped back on {port *<port>* | trunk *<trunk ID>*}
AMP	Discarding BPDUs received on port *<port>* while AMP is enabled
AMP	Dropping AMP v*<group>* packets received on {port *<port>* | trunk *<trunk ID>*}, expecting v*<AMP version>*
AMP	Port *<port>* is disabled by AMP BPDU guard
AMP	Putting port *<port>* in forwarding state
AMP	Putting port *<port>* in blocking state
BGP	Invalid notification (Code:*<code>*, Subcode:*<subcode>*) received from *<IP address>*
BGP	session with *<IP address>* failed (bad event:*<event>*)
BGP	session with *<IP address>* failed *<reason>* Reasons: • Connect Retry Expire • Receive UPDATE • Holdtime Expire • Start • Invalid • Stop • Keepalive Expire • Transport Conn Closed • Receive KEEPALIVE • Transport Conn Failed • Receive NOTIFICATION • Transport Conn Open • Receive OPEN • Transport Fatal Error

Thread	LOG_ALERT Message (continued)

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 • Invalid NEXTHOP Attr
	• Attr Flags Error • Invalid ORIGIN Attr
	• Attr Length Error • Malformed AS_PATH
	• Auth Failure • Malformed Attr List
	• Bad BGP Identifier • Missing Well Known Attr
	• Bad HoldTime • None
	• Bad Length • Optional Attr Error
	• Bad Peer AS • Unrecognized Well Known Attr
	• Bad Type
	• Conn Not Synced • Unsupported Opt Param
	• Invalid Network Field • 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 {MGTA | MGTB} port default gateway *<IP address>*
IP	Dynamic Routing table is full
IP	Route table full
MGMT	Maximum number of login failures (*<threshold>*) has been exceeded.
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

Thread	LOG_ALERT Message (continued)
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
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>
SYSTEM	link down on management port *<port>*
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	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	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	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
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>*
DCBX	Multiple peers detected on port *<port>*
IP6	EXCEPTIONAL CASE Trying to create IP6 Interface after the Ip6Shutdown
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

Thread	LOG_ERR Message (continued)
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 Erro. 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
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
PFC	PFC can be enabled on 2 priorities only - priority 3 and one other priority.
PORT_MIRR	ERROR: Management port *<port>* cannot be a mirrored port
RMON	Maximum {Alarm	Event	History} groups exceeded when trying to add group *<group>* via SNMP

Thread	LOG_ERR Message (continued)
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	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 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>*
MGMT	FLASH ERROR - invalid address used

Thread	LOG_INFO Message (continued)
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	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	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.
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	Starting Firmware download for {invalid image|image1|image2|boot kernel|undefined|SP boot kernel}.

Thread	LOG_INFO Message (continued)
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	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	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\>*
oflow	Openflow Statistics Cleared
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}

Thread	LOG_INFO Message (continued)
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>*
SYSTEM	Insert another transceiver or change configuration and manually enable port *<port>*

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	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>*
AMP	AMP group <group> topology is UP
AMP	Multiple LACP trunks using admin key <group> are currently active
AMP	Putting port *<port>* in forwarding state
BGP	bad authentication received / no authentication received / authentication receive error from *<IP address>*
BGP	session established with *<IP address>*
CFG	Note: The configured AMP interval and timeout-count values result in a very short keep-alive timeout that may lead to unstable topologies in some configurations. The suggested keep-alive timeout is at least *<value>* centisecond[s]
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>*

Thread	LOG_NOTICE Message (continued)
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.
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	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	{MGTA|MGTB} port default gateway *<IP address>* operational
IP	On Vlan *<VLAN>* IGMP version updated to *<version>*
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>*

Thread	LOG_NOTICE Message (continued)
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
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	MGTA | B 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 FIX-UP MODE IN USE
MGMT	Password for {oper | operator} changed by {SNMP user | *<username>*}, notifying admin to save.
MGMT	QSFP: Port *<port>* changed to {10G|40G}, from {BBI|SNMP|CLI}.
MGMT	RADIUS server timeouts

Thread	LOG_NOTICE Message (continued)
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
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
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}]

Thread	LOG_NOTICE Message (continued)
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>*}
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>* [via if *<interface>*] is {down | up}
SYSTEM	Enable auto negotiation for copper GIG port: *<port>*

Thread	LOG_NOTICE Message (continued)
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	link {down	up} on management port *<port>*
SYSTEM	Mask for interface *<interface>* ignored because of mismatch.
SYSTEM	**** MAX TEMPERATURE (*<temperature>*) ABOVE FAIL THRESH ****
SYSTEM	**** MAX TEMPERATURE (*<temperature>*) ABOVE WARN THRESH ****
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>*

Thread	LOG_NOTICE Message (continued)
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
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
UPGRADE	UFD couldn't be converted to Failover
UPGRADE	UpLinkFast is not supported in MSTP/RST/PVRST mode
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.

Thread	LOG_NOTICE Message (continued)
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.
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
AMP	Access port *<port>* is receiving AMP packets from access switch *<MAC address>*
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	Trunk hash changed, Dataplane L3 hash includes configured Trunk hash and ECMP hash
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.

Thread	LOG_WARNING Message (continued)
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>*
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
VNIC	Peer does not support VNIC on port *<port>*

Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- 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.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM *Documentation* CD that comes with your system.
- Go to the IBM support website at http://www.ibm.com/systems/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that 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.

Using the documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/systems/support/ and follow the instructions. Also, some documents are available through the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

Getting help and information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x® and xSeries® information is http://www.ibm.com/systems/x/. The address for IBM BladeCenter information is http://www.ibm.com/systems/bladecenter/. The address for IBM IntelliStation® information is http://www.ibm.com/intellistation/.

You can find service information for IBM systems and optional devices at http://www.ibm.com/systems/support/.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/, or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

> IBM Taiwan Corporation
> 3F, No 7, Song Ren Rd.
> Taipei, Taiwan
> Telephone: 0800-016-888

Index

Numerics

A

B

C

forwarding state
  (FWD) 44, 46
FWD (port state) 42
fwd (STP bridge option) 284
FwdDel (forward delay), bridge port 44, 46

G

gateway
  clearing routes that use 315
  default gateway configuration (IPv4) 314
  IPv6 398
getting help 497
gtcfg (TFTP load command) 432

H

hardware service and support 502
health checks
  default gateway interval, retries 314
  retry, number of failed health checks 314
hello (STP information) 43, 44, 45
help
  getting 497
  online 5
Hot Links configuration 303
hot-standby failover 389
HTTPS 242

I

IBM support line 501
ICMP
  statistics 155
idle timeout, setting 9
IEEE standards
  802.1x 42
IGMP
  configuration 365
  information 72
  multicast router information 75
  querier 371
  querier information 74
  snooping 366
  statistics 159
IKEv2
  configuration mode 4
  configuring 373
  identification, configuring 374
  information 85
  preshare keys 374
  proposal 373
image
  downloading 446
  software, selecting 447
indirect (IP route type) 53
information commands 11 to ??
interface change statistics 167, 171

IP address
  ARP information 54
  invalid (IPv4) 146
  invalid (IPv6) 149
IP forwarding
  directed broadcasts 319
  information 50
IP information 50, 83
IP interface 53
  active 391
  address of default gateway 314
  configuration mode 2
  configuring address 310
  configuring VLANs 310
  information 50
  IP route tag 53
  network filter configuration 320
  priority increment value (ifs) for VRRP 393
IP routing
  information 52
  information (IPv6) 69
  manipulation 464
  tag parameters 53
  tags 53
  types 53
IP Static Route commands 315
IPMC
  display all groups registered 143
  group information 76
IPsec
  configuring 375
  information 86
  Layer 3 configuration 348, 351
  traffic selector, configuring 377
  transform set, configuring 376
IPv4
  clear statistics 142
  route statistics 152
  statistics 146
IPv6
  ACL configuration 266
  clear statistics 142
  default gateway configuration 398
  ND prefix configuration 401
  Neighbor Discovery cache configuration 399
  Neighbor Discovery configuration 312
  Path MTU configuration 400
  Path MTU information 82
  re-mark configuration 269
  route information 69
  route statistics 153
  static route 399
  statistics 148
ISCLI commands
  basics 1 to 9
  modes 2

U

V

W