IBM Networking OS 7.5

ISCLI–Industry Standard CLI Command Reference

for the CN4093 10Gb Converged Scalable Switch

IBM Networking OS 7.5

ISCLI–Industry Standard CLI Command Reference

for the CN4093 10Gb Converged Scalable Switch

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.

First edition (November 2012)

Contents

Preface

This *ISCLI Command Reference* describes how to configure and use the IBM Networking OS 7.5 software with your IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch. 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 CN4093. For details about the configuration and operation of the CN4093, see the *IBM Networking OS 7.5 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, the IEEE 802.1D 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.

"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 {`***<1-64>***`|hash|information}`** you enter: **`show portchannel`** *<1-64>* or show **`portchannel`** hash or show **`portchannel`** information

Table 1. Typographic Conventions

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 ip interface [`***`<1-128>`***`]`** you enter **`show ip interface`** or **`show ip interface`** *<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 {`***`<1-64>`***`|hash|information}`** you must enter: **`show portchannel`** *<1-64>* or show **`portchannel`** hash or show **`portchannel`** information

How to Get Help

If you need help, service, or technical assistance, see the "Getting help and technical assistance" appendix in the *IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch User Guide*.

Chapter 1. ISCLI Basics

Your CN4093 10Gb Converged Scalable Switch (CN4093) 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 CN4093.

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.

Accessing the ISCLI

The first time you start the CN4093, it boots into IBM Networking OS CLI. To access the ISCLI, enter the following command and reset the CN4093:

```
Main# boot/mode iscli
```

To access the menu-based CLI, enter the following command from the ISCLI and reload the CN4093:

```
Router (config)# boot cli-mode ibmnos-cli
```

The switch retains your CLI selection, even when you reset the configuration to factory defaults. The CLI boot mode is not part of the configuration settings.

If you downgrade the switch software to an earlier release, it will boot into menu-based CLI. However, the switch retains the CLI boot mode, and will restore your CLI choice.

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 CN4093. 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 `Router>`	Default mode, entered automatically on console Exit: `exit` or `logout`
Privileged EXEC `Router#`	Enter Privileged EXEC mode, from User EXEC mode: `enable` Exit to User EXEC mode: `disable` Quit ISCLI: `exit` or `logout`
Global Configuration `Router(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: `configure terminal` Exit to Privileged EXEC: `end` or `exit`
Interface IP `Router(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 `Router(config-ip-loopback)#`	Enter Interface Loopback Configuration mode, from Global Configuration mode: `interface ip loopback` <*1-5*> Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Interface Port `Router(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 `Router(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`

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
VLAN `Router(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 `Router(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 BGP `Router(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 `Router(config-router-rip)#`	Enter RIP Configuration mode, from Global Configuration mode: `router rip` Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Route Map `Router(config-route-map)#`	Enter Route Map Configuration mode, from Global Configuration mode: `route-map` *<1-32>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
Router VRRP `Router(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 `Router(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`

Table 2. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
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`
VSI Database `CN4093(conf-vsidb)#`	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: `virt evb vsidb` *<VSIDB_number>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
EVB Profile `CN4093(conf-evbprof)#`	Enter Edge Virtual Bridging VSI Type Profile Configuration mode, from Global Configuration mode: `virt evb profile` *<1-16>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
FC Port Configuration `CN4093(config-fc)#`	Enter Fibre Channel Port Configuration mode, from Global Configuration mode: `interface fc` *<port alias or number>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
FC Zone Configuration `CN4093(config-zone)#`	Enter Fibre Channel Zone Configuration mode, from Global Configuration mode: `zone name` *<1-64 characters>* Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
FC Zoneset Configuration `CN4093(config-zoneset)#`	Enter Fibre Channel Zoneset Configuration mode, from Global Configuration mode: `zoneset name` *<1-64 characters>* 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>*`]` `[-v` *<tos (0-255)>*`]` `[-f]` `[-t]` 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). – `-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`). Where the *IP address* or *hostname* specify the target device. Use of a hostname requires DNS parameters to be configured on the switch. *Tries* (optional) is the number of attempts (1-32), and *msec delay* (optional) is the number of milliseconds between attempts.

Table 3. Description of Global Commands (continued)

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*>]] `traceroute` <*hostname*>|<*IP address*> [<*max-hops (1-32)*> [<*msec-delay (1-4294967295)*>]] 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. 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*>] 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.
`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 1,3,4095                    (access VLANs 1, 3, and 4095)
# vlan 1-20                        (access VLANs 1 through 20)
# vlan 1-5,90-99,4090-4095         (access multiple ranges)
# vlan 1-5,19,20,4090-4095         (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:

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

or

```
Router(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.

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the CN4093. 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 CN4093. 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 CN4093. 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 CN4093. 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 CN4093 10Gb Converged Scalable Switch, 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 speed – Duplex mode (half, full, or auto) – Flow control for transmit and receive (no, yes, or both) – Link status (up, down, or disabled) For details, see page 99. **Command mode:** All
`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 name – VLAN membership – FDB Learning status – Flooding status For details, see page 100. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each external port. For details, see page 101. **Command mode:** All
`show software-key` Displays the enabled software features.
`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 on page 16, with pointers to where detailed information can be found.

Table 6. System Information Commands

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 For details, see page 26. **Command mode:** All
`show logging` Displays most recent syslog messages, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 27. **Command mode:** All
`show access user` Displays configured user names and their status. **Command mode:** Privileged EXEC

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 Commands

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

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 Commands

Command Syntax and Usage
`show snmp-server v3 user` Displays User Security Model (USM) table information. To view the table, see page 19. **Command mode:** All
`show snmp-server v3 view` Displays information about view, subtrees, mask and type of view. To view a sample, see page 20. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 21. **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 22. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 22. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 23. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 23. **Command mode:** All
`show snmp-server v3 notify` Displays the Notify table information. To view a sample, see page 24. **Command mode:** All
`show snmp-server v3` Displays all the SNMPv3 information. To view a sample, see page 25. **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

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

Table 10. USM User Table Information Parameters

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. IBM Networking OS supports DES algorithm for privacy. The software also supports 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 sub system 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

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

```
Sec Model    User Name                       Group Name
----------   ------------------------------  --------------------
snmpv1       v1v2only                        v1v2grp
usm          adminmd5                        admingrp
usm          adminsha                        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

This command displays the community table information stored in the SNMP engine.

The following command displays SNMPv3 community information:

```
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:

```
show snmp-server v3 target-address
```

Command mode: All

This command displays the SNMPv3 target address table information, which is stored in the SNMP engine.

```
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 which 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

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

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

vacmViewTreeFamily Table:
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

vacmSecurityToGroup Table:
Sec Model  User Name                        Group Name
---------- -------------------------------  ----------------------
snmpv1     v1v2only                         v1v2grp
usm        adminsha                         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 0:16:42 Wed Jan 3, 2012
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled
IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot:  0:00:47 Wed Jan  3, 2012 (reset from console)

MAC address: 00:17:ef:4a:9f:00    IP (If 1) address: 0.0.0.0
Internal Management Port MAC Address: 00:00:00:00:00:ef
Internal Management Port IP Address (if 128): 9.43.95.121
External Management Port MAC Address: 00:00:00:00:00:fe
External Management Port IP Address (if 127):
Software Version 7.5.0 (FLASH image2), active configuration.

Hardware Part Number        : 49Y4272
Hardware Revision:     05
Serial Number:         PROTO2C04E
Manufacturing Date:    43/08
PCBA Part Number:      BAC-00072-00
PCBA Revision:         0
PCBA Number:           00
Board Revision:        05
PLD Firmware Version:  1.3

Temperature Warning:   26 C (Warn at 60 C/Recover at 55 C)
Temperature Shutdown:  27 C (Shutdown at 65 C/Recover at 60 C)
Temperature Inlet:     23 C
Temperature Exhaust:   26 C

Power Consumption:     42.570 W (12.000 V,  3.543 A)

Switch is in I/O Module Bay 1
```

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

Show Software Version Information

The following command displays the software version number, image file, and configuration name:

```
show version brief
```

Command mode: All

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

```
Date    Time      Criticality level       Message
Jul  8  17:25:41    NOTICE       system: link up on port INTA1
Jul  8  17:25:41    NOTICE       system: link up on port INTA8
Jul  8  17:25:41    NOTICE       system: link up on port INTA7
Jul  8  17:25:41    NOTICE       system: link up on port INT2
Jul  8  17:25:41    NOTICE       system: link up on port INTA1
Jul  8  17:25:41    NOTICE       system: link up on port INT4
Jul  8  17:25:41    NOTICE       system: link up on port INTA3
Jul  8  17:25:41    NOTICE       system: link up on port INTA6
Jul  8  17:25:41    NOTICE       system: link up on port INTA5
Jul  8  17:25:41    NOTICE       system: link up on port EXT4
Jul  8  17:25:41    NOTICE       system: link up on port EXT1
Jul  8  17:25:41    NOTICE       system: link up on port EXT3
Jul  8  17:25:41    NOTICE       system: link up on port EXT2
Jul  8  17:25:41    NOTICE       system: link up on port INTA3
Jul  8  17:25:42    NOTICE       system: link up on port INTA2
Jul  8  17:25:42    NOTICE       system: link up on port INTA4
Jul  8  17:25:42    NOTICE       system: link up on port INTA3
Jul  8  17:25:42    NOTICE       system: link up on port INTA6
Jul  8  17:25:42    NOTICE       system: link up on port INTA5
```

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 below.

- `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

The following commands display Layer 2 information.

Table 18. Layer 2 Information Commands

Command Syntax and Usage
`show dot1x information` Displays 802.1X Information. **Command mode:** All For details, see page 40.
`show spanning-tree` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (PVRST, RSTP, 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 stp <1-128> information` Displays information about a specific Spanning Tree Group. **Command mode:** All For details, see page 42.

Table 18. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show spanning-tree mstp cist information` Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership. 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 47. **Command mode:** All
`show portchannel information` Displays the state of each port in the various static or LACP trunk groups. For details, see page 49. **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 50. **Command mode:** All
`show failover trigger` <*trigger number*> Displays Layer 2 Failover information. For details, see page 33. **Command mode:** All

Table 18. Layer 2 Information Commands (continued)

Command Syntax and Usage
`show hotlinks information` Displays Hot Links information. For details, see page 34. **Command mode:** All
`show layer2 information` Dumps all Layer 2 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

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 K MAC address entries on the MP per switch.

Table 19. FDB Information Commands

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 interface 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

Table 19. FDB Information Commands (continued)

Command Syntax and Usage
`show mac-address-table multicast` Displays all Multicast MAC entries in the FDB. **Command mode:** All
`show mac-address-table static` Displays all static 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` Displays all entries in the Forwarding Database. **Command mode:** All For more information, see page 31.

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  EXT4         FWD
 00:09:6b:9b:01:5f     1  INTA13       FWD
 00:09:6b:ca:26:ef  4095  MGT1         FWD
 00:0f:06:ec:3b:00  4095  MGT1         FWD
 00:11:43:c4:79:83     1  EXT4         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 will be listed under “Reference ports.”

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to “Forwarding Database Maintenance” on page 448.

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the CN4093.

Table 20. LACP Information Commands

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. **Command mode:** All For details, see page 32.

Link Aggregation Control Protocol

The following command displays LACP information:

```
show lacp information
```

Command mode: All

```
port   mode     adminkey  operkey  selected   prio  aggr  trunk  status  minlinks
-------------------------------------------------------------------------------
INTA1  active         30       30     yes    32768    17     19    up        1
INTA2  active         30       30     yes    32768    17     19    up        1
INTA3  off             3        3     no     32768    --     --    --        1
INTA4  off             4        4     no     32768    --     --    --        1
...
```

LACP dump includes the following information for each external port in the CN4093:

- `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 or down).
- `minlinks` Displays the minimum number of links required to establish a trunk.

Layer 2 Failover Information

Table 21. Layer 2 Failover Information Commands

Command Syntax and Usage
`show failover trigger` *<trigger number>* Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All
`show failover trigger` Displays a summary of Layer 2 Failover information. For details, see page 33. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

```
show failover trigger
```

Command mode: All

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
trunk 1
 EXT2       Operational
 EXT3       Operational

Control State: Auto Disabled
Member      Status
---------   -----------
 INTA1      Operational
 INTA2      Operational
 INTA3      Operational
 INTA4      Operational
...
```

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 the above 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
bpdu disabled
sndfdb disabled

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

Active state: None

Master settings:
port EXT1
Backup settings:
port EXT2
```

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

Edge Control Protocol Information

Table 22. ECP Information Options

Command Syntax and Usage
`show ecp channels` Displays all Edge Control Protocol (ECP) channels. **Command mode:** All
`show ecp upper-layer-protocols` Displays all registered Upper-Level Protocols (ULPs). **Command mode:** All

LLDP Information

The following commands display LLDP information.

Table 23. LLDP Information Commands

Command Syntax and Usage
`show lldp port` 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` Displays information received from LLDP -capable devices. To view a sample display, see page 35.
`show lldp port <1-16> tlv evb` Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information. **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

LocalPort | Index | Remote Chassis ID | RemotePort | Remote System Name
----------|-------|------------------|------------|--------------------------
     MGT1 | 210   | 00 16 ca ff 7e 00 | 15         | BNT Gb Ethernet Switch...
     EXT4 | 15    | 00 16 60 f9 3b 00 | 20         | BNT Gb Ethernet Switch...
```

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: EXT1
        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        : EXT1

        System Name        :
        System Description : IBM Networking Operating System CN4093 10Gb Converged
Scalable Switch, IBM Networking OS: version 7.5.0,45 Boot image: version 7.5.0.45

        System Capabilities Supported : bridge, router
        System Capabilities Enabled   : bridge, router

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

Unidirectional Link Detection Information

The following commands show unidirectional link detection information.

Table 24. UDLD Information Commands

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 EXT1
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: EXT1
```

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 25. OAM Discovery Information Commands

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 EXT1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

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

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

vLAG Information

The following table lists the information commands for Virtual Link Aggregation Group (vLAG) protocol.

Table 26. vLAG Information Options

Command Syntax and Usage
`show vlag adminkey` *<1-65535>* Displays vLAG LACP information. **Command mode:** All
`show vlag portchannel` *<trunk group number>* Displays 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 3
Protocol - Static
Current settings: enabled
    ports:  60
Current L2 trunk hash settings:
    smac
Current L3 trunk hash settings:
    sip dip
Current ingress port hash: disabled
Current L4 port hash: disabled
```

802.1X Information

The following command displays 802.1X information:

```
show dot1x information
```

Command mode: All

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
Guest VLAN status : disabled
Guest VLAN        : none
                                    Authenticator    Backend   Assigned
Port    Auth Mode    Auth Status     PAE State     Auth State   VLAN
-----  ------------  ------------  --------------  ---------- --------
*INTA1 force-auth    unauthorized  initialize      initialize   none
*INTB1 force-auth    unauthorized  initialize      initialize   none
*INTC1 force-auth    unauthorized  initialize      initialize   none
*INTA2 force-auth    unauthorized  initialize      initialize   none
*INTB2 force-auth    unauthorized  initialize      initialize   none
*INTC2 force-auth    unauthorized  initialize      initialize   none
...
*EXT1  force-auth    unauthorized  initialize      initialize   none
*EXT2  force-auth    unauthorized  initialize      initialize   none
*EXT3  force-auth    unauthorized  initialize      initialize   none
*EXT4  force-auth    unauthorized  initialize      initialize   none
...
------------------------------------------------------------------
* - Port down or disabled
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System unit that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

Table 27. 802.1X Parameter Descriptions

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: – force-unauth – auto – force-auth
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.

Table 27. 802.1X Parameter Descriptions (continued)

Parameter	Description
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: – initialize – disconnected – connecting – authenticating – authenticated – aborting – held – forceAuth
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: – initialize – request – response – success – fail – timeout – idle

Spanning Tree Information

The following command displays Spanning Tree information:

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

Command mode: All

```
------------------------------------------------------------------
Pvst+ compatibility mode enabled
------------------------------------------------------------------
Spanning Tree Group 1: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 ffff 00:13:0a:4f:7d:d0        0    EXT2    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology Change Counts
              65535      2      20      15     300               0

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
INTA1  128     2000!  FWD   ROOT 8000-00:22:00:ee:cc:00     8001  P2P
INTA2  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8002  P2P
INTA3  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8003  P2P
...
EXT1  128     2000!  DISC  DESG 8001-00:22:00:7d:5f:00     800a  P2P
EXT2  128     2000!  DISC  DESG 8001-00:22:00:7d:5f:00     800b  P2P
...
! = Automatic path cost.

------------------------------------------------------------------
Spanning Tree Group 128: Off (PVRST), FDB aging timer 300
VLANs:  4095

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
EXTM             0        0    FWD *
MGT1             0        0    FWD *
* = STP turned off for this port.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis that you are using and the firmware versions and options that are installed.

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) Spanning Tree mode, with IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), as alternatives. For details, see “RSTP/MSTP/PVRST Information” on page 44.

When STP is enabled, in addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

Table 28. Spanning Tree Bridge Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root.
Priority (bridge)	The Bridge Priority parameter controls which bridge on the network will become the STG root bridge.
Hello	The Hello Time parameter specifies, in seconds, how often the root 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 STG network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

The following port-specific information is also displayed:

Table 29. Spanning Tree 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 `FWD` (Forwarding), `DISC` (Discarding) or `LRN` (Learning).
Role	The role field shows the current role of the port : DESG (Designated), `ROOT` (Root Port), `ALTN` (Alternate) or `BKUP` (Backup).

Table 29. Spanning Tree 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.

RSTP/MSTP/PVRST Information

The following command displays RSTP/MSTP/PVRST information:

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

Command mode: All

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

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 ffff 00:13:0a:4f:7d:d0        0    EXT4     2    20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              61440      2      20      15     300

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
INTA1  128     2000!  FWD   ROOT 8000-00:22:00:ee:cc:00     8001  P2P
INTA2  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8002  P2P
INTA3  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8003  P2P
...
EXT1   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8011     P2P
EXT2   128      2000  DISC  BKUP 8000-00:11:58:ae:39:00    8011     P2P
EXT3   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8013     P2P
EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8013  Shared
EXT5   128      2000  FWD
...
------------------------------------------------------------------
Spanning Tree Group 128: Off (RSTP), FDB aging timer 300
VLANs:  4095

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
EXTM             0        0    FWD *
MGT1             0        0    FWD *

* = STP turned off for this port.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis that you are using and the firmware versions and options that are installed.

You can configure the switch software to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST).

If RSTP/MSTP/PVRST is turned on, you can view the following bridge information for the Spanning Tree Group:.

Table 30. RSTP/MSTP/PVRST Bridge Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the 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 root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

The following port-specific information is also displayed:

Table 31. RSTP/MSTP/PVRST Port Parameter Descriptions

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

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

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

Common Internal Spanning Tree Information

The following command displays Common Internal Spanning Tree (CIST) information:

```
show spanning-tree mstp cist information
```

Command mode: All

```
Common Internal Spanning Tree: on
VLANs:  2-4094

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

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

Parameters:  Priority  MaxAge  FwdDel  Hops
              61440      20      15    20
Port  Prio  Cost     State  Role Designated Bridge      Des Port Hello Type
----- ---- --------- -----  ---- ---------------------- -------- ----- ----
 INTA1    0         0  DSB *
 INTA2    0         0  DSB *
 INTA3    0         0  FWD *
 INTA4    0         0  DSB *
 INTA5    0         0  DSB *
 INTA6    0         0  DSB *
 INTA7    0         0  DSB *
 INTA8    0         0  DSB *
 INTA9    0         0  DSB *
 INTA10   0         0  DSB *
 INTA11   0         0  DSB *
 INTA12   0         0  DSB *
 INTA13   0         0  DSB *
 INTA14   0         0  DSB *
 MGT1     0         0  FWD *
*EXT1   128     20000  FWD   DESG 8000-00:11:58:ae:39:00    8011   2    P2P
 EXT2   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8011   2    P2P
 EXT3   128     20000  FWD   DESG 8000-00:11:58:ae:39:00    8013   2    P2P
 EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8013   2    Shared
...
* = STP turned off for this port.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis that you are using and the firmware versions and options that are installed.

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view the following CIST bridge information:

Table 32. 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 root 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.
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 33. 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`).

Table 33. CIST Parameter Descriptions (continued)

Parameter	Description
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`), Backup (`BKUP`), 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:
  EXT1: STG  1 forwarding
  EXT2: 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 34. VLAN Information Commands

Command Syntax and Usage
`show vlan` *<VLAN number>* Displays general VLAN information.
`show protocol-vlan` *<protocol number>* Displays protocol VLAN information. **Command mode:** All
`show private-vlan` *<VLAN number>* Displays private VLAN information. **Command mode:** All
`show vlan information` Displays information about all VLANs, including: – VLAN number and name – Port membership – VLAN status (enabled or disabled) – Protocol VLAN status – Private VLAN status – Spanning Tree membership – VMAP configuration

The following command displays VLAN information:

```
show vlan
```

Command mode: All

```
VLAN                Name                 Status MGT           Ports
----  --------------------------------  ------ --- -------------------------
1     Default VLAN                      ena    dis  INTA1-INTB14 EXT1-EXT10
                                                     EXT15-EXT22
4095  Mgmt VLAN                         ena    ena  MGT1 EXTM
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis that you are using and the firmware versions and options that are installed.

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 Type
- Status

- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

Layer 3 Information

Table 35. Layer 3 Information Commands

Command Syntax and Usage
`show ip route` Displays all routes configured on the switch. For details, see page 55. **Command mode:** All
`show arp` Displays Address Resolution Protocol (ARP) information. For details, see page 56. **Command mode:** All
`show ip bgp information` Displays Border Gateway Protocol (BGP) information. For details, see page 60. **Command mode**: All
`show ip ospf information` Displays the OSPF information. For more OSPF information options, see page 61. **Command mode**: All
`show ipv6 ospf information` Displays OSPFv3 information. For more OSPFv3 information options, see page 66. **Command mode**: All
`show ip rip interface` Displays RIP user's configuration. For details, see page 70. **Command mode**: All
`show ipv6 route` Displays IPv6 routing information. For more information options, see page 71. **Command mode**: All
`show ipv6 neighbors` Displays IPv6 Neighbor Discovery cache information. For more information options, see page 73. **Command mode**: All
`show ipv6 prefix` Displays IPv6 Neighbor Discovery prefix information. For details, see page 74. **Command mode**: All
`show ip ecmp` Displays ECMP static route information. For details, see page 74. **Command mode**: All

Table 35. Layer 3 Information Commands (continued)

Command Syntax and Usage
`show ip igmp groups` Displays IGMP Information. For more IGMP information options, see page 76. **Command mode**: All
`show ipv6 mld groups` Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see page 79. **Command mode**: All
`show ip vrrp information` Displays VRRP information. For details, see page 81. **Command mode:** All
`show interface ip` Displays IPv4 interface information. For details, see page 82. **Command mode:** All
`show ipv6 interface` <*interface number*> Displays IPv6 interface information. For details, see page 82. **Command mode:** All
`show ipv6 pmtu [`<*destination IPv6 address*>`]` Displays IPv6 Path MTU information. For details, see page 83. **Command mode:** All
`show ip interface brief` Displays IP Information. For details, see page 84. 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 page 85. **Command mode:** All
`show ipsec manual-policy` Displays information about manual key management policy for IP security. For more information options, see page 86. **Command mode:** All

Table 35. Layer 3 Information Commands (continued)

Command Syntax and Usage
`show ip pim component [<1-2>]` Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see page 87. **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 prior to issuing the dump commands. **Command mode:** All

IP Routing Information

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

Table 36. Route Information Commands

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 37 on page 55. **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 38 on page 56. **Command mode:** All
`show ip route interface <interface number>` Displays routes on a single interface. **Command mode:** All

Table 36. Route Information Commands (continued)

Command Syntax and Usage
`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 55.

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
 --------------- --------------- --------------- --------- --------- ---- ---
* 12.0.0.0        255.0.0.0       11.0.0.1        direct    fixed         128
* 12.0.0.1        255.255.255.255 11.0.0.1        local     addr          128
* 12.255.255.255  255.255.255.255 11.255.255.255  broadcast broadcast     128
* 12.0.0.0        255.0.0.0       12.0.0.1        direct    fixed          12
* 12.0.0.1        255.255.255.255 12.0.0.1        local     addr           12
* 255.255.255.255 255.255.255.255 12.255.255.255  broadcast broadcast       2
* 224.0.0.0       224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.5       255.255.255.255 0.0.0.0         multicast addr
```

The following table describes the `Type` parameters.

Table 37. 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 38. 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 CN4093 10Gb Converged Scalable Switch.
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)
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 40 on page 57), VLAN and port for the address, and port referencing information.

Table 39. ARP Information Commands

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

Table 39. ARP Information Commands (continued)

Command Syntax and Usage
`show arp` Displays all ARP entries. including: – IP address and MAC address of each entry – Address status flag (see below) – 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 57. **Command mode:** All
`show arp reply` Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags. **Command mode:** All

Show All ARP Entry Information

The following command displays ARP information:

```
show arp
```

Command mode: All

```
    IP address     Flags    MAC address    VLAN  Age Port
---------------- ----- ----------------- ----  --- -----
12.20.1.1             00:15:40:07:20:42 4095    0  INT8
12.20.20.16           00:30:13:e3:44:14 4095    2  INT8
12.20.20.18           00:30:13:e3:44:14 4095    2  INT6
12.20.23.111          00:1f:29:95:f7:e5 4095    6  INT6
```

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

The `Flags` field is interpreted as follows:

Table 40. ARP Dump 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.

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 Flags
--------------- --------------- ----------------- ---- -----
205.178.18.66   255.255.255.255  00:70:cf:03:20:04        P
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
```

BGP Information

Table 41. BGP Peer Information Commands

Command Syntax and Usage
`show ip bgp neighbor information` Displays BGP peer information. See page 59 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 60 for a sample output. **Command mode:** All
`show ip bgp aggregate-address` Displays BGP peer routes. See page 60 for a sample output. **Command mode:** All
`show ip bgp information` Displays the BGP routing table. See page 60 for a sample output. **Command mode:** All

BGP Peer information

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

```
show ip bgp neighbor information
```

Command mode: All

```
BGP Peer Information:

  3: 2.1.1.1         , version 4, TTL 225
    Remote AS: 100, Local AS: 100, Link type: IBGP
    Remote router ID: 3.3.3.3,    Local router ID: 1.1.201.5
    BGP status: idle, Old status: idle
    Total received packets: 0, Total sent packets: 0
    Received updates: 0, Sent updates: 0
    Keepalive: 60, Holdtime: 180, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 1

  4: 2.1.1.4         , version 4, TTL 225
    Remote AS: 100, Local AS: 100, Link type: IBGP
    Remote router ID: 4.4.4.4,    Local router ID: 1.1.201.5
    BGP status: idle, Old status: idle
    Total received packets: 0, Total sent packets: 0
    Received updates: 0, Sent updates: 0
    Keepalive: 60, Holdtime: 180, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 1
```

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
```

BGP Peer Routes Information

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

```
show ip bgp aggregate-address
```

Command mode: All

```
Current BGP neighbor 1 routes:
 Status codes: * valid, > best, = multipath, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network         Mask            Next Hop        Metr LcPrf  Wght  Path
   --------------- --------------- --------------- ----- ----- ----- --------------
*> 157.0.0.0       255.255.255.0   200.0.0.2         256    4    10   i
*> 157.0.1.0       255.255.255.0   200.0.0.2         256    4    10   i
*> 157.0.2.0       255.255.255.0   200.0.0.2         256    4    10   i
*> 157.0.3.0       255.255.255.0   200.0.0.2         256    4    10   i
*> 157.0.4.0       255.255.255.0   200.0.0.2         256    4    10   i
*> 157.0.5.0       255.255.255.0   200.0.0.2         256    4    10   i
```

Dump BGP Information

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

```
show ip bgp information
```

Command mode: All

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

The 13.0.0.0 is filtered out by rrmap; or, a loop detected.
```

OSPF Information

Table 42. OSPF Information Commands

Command Syntax and Usage
`show ip ospf general-information` Displays general OSPF information. **Command mode:** All See page 62 for a sample output.
`show ip ospf area information` Displays area information for all areas. **Command mode:** All
`show ip ospf area <0-2>` Displays area information for a particular area index. **Command mode:** All
`show ip ospf interface loopback <1-5>` Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces. See page 63 for a sample output. **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 63 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 <0-2>` Displays the list of summary ranges belonging to non-NSSA areas. **Command mode:** All
`show ip ospf summary-range-nssa <0-2>` Displays the list of summary ranges belonging to NSSA areas. **Command mode:** All

Table 42. OSPF Information Commands (continued)

Command Syntax and Usage
`show ip ospf routes` Displays OSPF routing table. See page 65 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 Loopback Information

The following command displays OSPF interface loopback information:

`show ip ospf interface loopback <interface number>`

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 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,
   Neighbor count is 1   If Events 4, Authentication type none
```

OSPF Database Information

Table 43. OSPF Database Information Commands

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 43. OSPF Database Information Commands (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 44. OSPFv3 Information Options

Command Syntax and Usage
`show ipv6 ospf area` *<area index (0-2)>* Displays the area information. **Command mode:** All
`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 68. **Command mode:** All
`show ipv6 ospf area-virtual-link` 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` 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
`show ipv6 ospf redist-config` Displays OSPFv3 redistribution information to be applied to routes learned from the route table. **Command mode:** All

Table 44. OSPFv3 Information Options

Command Syntax and Usage
`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 page 70. **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 page 68. **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 45. 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

Table 45. OSPFv3 Database Information Options

Command Syntax and Usage
`show ipv6 ospf database inter-router [detail|hex]` Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
`show ipv6 ospf database intra-prefix [detail|hex]` Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
`show ipv6 ospf database link [detail|hex]` Displays Link LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
`show ipv6 ospf database network [detail|hex]` Displays Network LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
`show ipv6 ospf database 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 database 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 46. Routing Information Protocol Commands

Command Syntax and Usage
`show ip rip routes` Displays RIP routes. **Command mode:** All For more information, see page 70.
`show ip rip interface` *<interface number>* Displays RIP user's configuration. **Command mode:** All For more information, see page 71.

RIP Routes Information

The following command displays RIP route information:

```
show ip rip routes
```

Command mode: All

```
Router(config)

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 1 : 10.4.4.2,         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 47 describes the IPv6 Routing information options.

Table 47. IPv6 Routing Information Commands

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 37 on page 55.
`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 72.

IPv6 Routing Table

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
        M - Management Gateway, 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]
        via ::, Interface 2
```

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

IPv6 Neighbor Discovery Cache Information

Table 48. IPv6 Neighbor Discovery Cache Information Commands

Command Syntax and Usage
`show ipv6 neighbors find` *<IPv6 address>* Shows a single IPv6 Neighbor Discovery cache entry by IP address. **Command mode:** All
`show ipv6 neighbors interface port` *<port alias or number>* Shows IPv6 Neighbor Discovery cache entries on a single port. **Command mode:** All
`show ipv6 neighbors vlan` *<VLAN number>* Shows IPv6 Neighbor Discovery cache entries on a single VLAN. **Command mode:** All
`show ipv6 neighbors static` Displays static IPv6 Neighbor Discovery cache entries. **Command mode:** All
`show ipv6 neighbors` Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 73. **Command mode:** All

IPv6 Neighbor Discovery Cache Information

The following command displays a summary of IPv6 Neighbor Discovery 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     EXT1
fe80::250:bfff:feb7:76b0   0   00:50:bf:b7:76:b0 Stale     2   1     EXT2
```

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
                                10.234.4.4        1    up
                                10.235.5.5        1    up
```

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

ECMP Hashing Result

The following command displays the status of ECMP hashing on each switch:

```
show ip route ecmp hash
```

Command mode: All

```
Enter SIP address: 10.0.0.1
Enter DIP address (0 for SIP only): 10.0.0.2
Enter number of ECMP paths: 3
Source 10.0.0.1 will go through route number 3
```

IGMP Multicast Group Information

Table 49. IGMP Multicast Group Information Commands

Command Syntax and Usage
`show ip igmp querier vlan` *<VLAN number>* Displays IGMP Querier information. For details, see page 77. **Command mode:** All
`show ip igmp snoop` Displays IGMP Snooping information. **Command mode:** All
`show ip igmp relay` Displays IGMP Relay information. **Command mode:** All
`show ip igmp mrouter information` Displays IGMP Multicast Router information. **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 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
`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

Table 49. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage
`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. **Command mode:** All

IGMP Querier Information

The following command displays IGMP Querier information:

`show ip igmp querier vlan <VLAN number>`

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 0.0.0.0,
 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

```
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Source         Group       VLAN    Port   Version   Mode  Expires  Fwd
 -------------- --------------- ------- ------ --------  ----- -------  ---
 10.1.1.1       232.1.1.1        2      EXT4    V3       INC    4:16    Yes
 10.1.1.5       232.1.1.1        2      EXT4    V3       INC    4:16    Yes
    *           232.1.1.1        2      EXT4    V3       INC     -      No
 10.10.10.43    235.0.0.1        9      EXT1    V3       INC    2:26    Yes
    *           236.0.0.1        9      EXT1    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

```
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        -       -
10.10.10.43         9       24         V2          -        -        -       -
```

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 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 50 describes the commands used to view Multicast Listener Discovery (MLD) information.

Table 50. MLD Information Commands

Command Syntax and Usage
`show ipv6 mld groups` Displays MLD multicast group information. **Command mode:** All
`show ipv6 mld groups address` <*IPv6 address*> Displays group information for the specified IPv6 address. **Command mode:** All
`show ipv6 mld groups interface port` <*port alias or number*> Displays MLD groups on a single interface port. **Command mode:** All
`show ipv6 mld groups portchannel` <*trunk group number*> Displays groups on a single port channel. **Command mode:** All

Table 50. MLD Information Commands

Command Syntax and Usage
`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 80 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 51. 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 CN4093 10Gb Converged Scalable Switch 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:
126: IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::a17:f4ff:fe0a:1ef
127: IP4 10.43.98.33      255.255.255.0   9.43.98.255,     vlan 4095, up
128: IP4 10.43.95.162     255.255.255.0   9.43.95.255,     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)

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:
  AS number 0

Interface information:
126: IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::200:ff:fe00:ef
128: IP4 9.43.95.121     255.255.255.0   9.43.95.255,     vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  4: 9.43.95.254,     FAILED

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 IP forwarding settings: ON, dirbr disabled, icmprd 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 52. IKEv2 Information Commands

Command Syntax and Usage
`show ikev2` Displays all IKEv2 information. See page 85 for sample output.
`show ikev2 ca-cert` Displays the CA certificate.
`show ikev2 host-cert` Displays the host certificate.
`show ikev2 identity` Displays IKEv2 identity information.
`show ikev2 preshare-key` Displays the IKEv2 preshare key.
`show ikev2 proposal` Displays the IKEv2 proposal.
`show ikev2 retransmit-interval` Displays the IKEv2 retransmit interval.
`show ikev2 sa` Displays the IKEv2 SA.

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 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.

IPsec Information

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

Table 53. IPsec Information Commands

Command Syntax and Usage
`show ipsec sa` Displays all security association information.
`show ipsec spd` Displays all security policy information.
`show ipsec dynamic-policy <1-10>` Displays dynamic policy information.
`show ipsec manual-policy <1-10>` Displays manual policy information. See page 87 for sample output.
`show ipsec transform-set <1-10>` Displays IPsec transform set information.
`show ipsec traffic-selector <1-10>` Displays IPsec traffic selector information.

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

PIM Information

Table 54. 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 89. **Command mode:** All
`show ip pim interface [<interface number>]|detail|loopback` Displays PIM interface information. To view sample output, see page 89. **Command mode:** All

Table 54. PIM Information Options (continued)

Command Syntax and Usage
`show ip pim neighbor [<`*interface number*`>]` Displays PIM neighbor information. To view sample output, see page 90. **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*`>|`
`source <`*multicast source address*`>`
Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see page 90.
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
`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 55. 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>` Displays PIM multicast routes for the selected incoming IP interface. **Command mode:** All

Table 55. PIM Multicast Route Information Options (continued)

Command Syntax and Usage
`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 56. 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 page 92.
`show qos random-detect` Displays WRED ECN information. **Command mode:** All For details, see page 92.

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
-----  --------  ----  ------
INTA1        0       0      1
INTA2        0       0      1
...
MGT1         0       0      1
EXT1         0       0      1
EXT2         0       0      1
EXT3         0       0      1
EXT4         0       0      1
...
```

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

Table 57. 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 58. 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 Commands

Table 59. ACL Information Options

Command Syntax and Usage
`show access-control list` *<ACL number>* Displays ACL list information. For details, see page 94. **Command mode:** All
`show access-control list6` *<ACL number>* Displays IPv6 ACL list information. **Command mode:** All
`show access-control group` *<ACL group number>* Displays ACL group 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 information:
------------------------
  Filter 2 profile:
   Ethernet
     - VID        : 2/0xfff
   Actions        : Permit
   Statistics     : enabled
```

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

Table 60. ACL Parameter Descriptions

Parameter	Description
Filter *x* profile	Indicates the ACL number.
Actions	Displays the configured action for the ACL.
Statistics	Displays the status of ACL statistics configuration (enabled or disabled).

RMON Information Commands

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

Table 61. RMON Information commands

Command Syntax and Usage
`show rmon history` Displays RMON History information. For details, see page 95. **Command mode:** All
`show rmon alarm` Displays RMON Alarm information. For details, see page 96. **Command mode:** All
`show rmon event` Displays RMON Event information. For details, see page 97. **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 62. RMON History Parameter Descriptions

Parameter	Description
Index	Displays the index number that identifies each history instance.
IFOID	Displays the MIB Object Identifier.

Table 62. RMON History Parameter Descriptions (continued)

Parameter	Description
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 63. 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.

Table 63. RMON Alarm Parameter Descriptions (continued)

Parameter	Description
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.
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 Alarm 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 64. 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       Name
------- ----   -----   --------  --TX-----RX--   ------     ------
INTA1   1      1G/10G    full     yes    yes      down       INTA1
INTA2   2      1G/10G    full     yes    yes      down       INTA2
INTA3   3      1G/10G    full     yes    yes      down       INTA3
INTA4   4      1G/10G    full     yes    yes      down       INTA4
...
INTA14  14     1G/10G    full     yes    yes      down       INTA14
INTB1   15     1G/10G    full     yes    yes      down       INTB1
INTB2   16     1G/10G    full     yes    yes      down       INTB2
INTB3   17     1G/10G    full     yes    yes      down       INTB3
INTB4   18     1G/10G    full     yes    yes      down       INTB4
...
INTC14  42     1G/10G    full     yes    yes      down       INTC14
EXT1    43     1G/10G    full      no     no      down       EXT1
EXT2    44     1G/10G    full      no     no      down       EXT2
EXT3    45     10000     full      no     no       up        EXT3
EXT4    46     1G/10G    full      no     no      down       EXT4
...
EXT20   62     10000     full      no     no    disabled     EXT20
EXT21   63     10000     full      no     no    disabled     EXT21
EXT22   64     10000     full      no     no    disabled     EXT22
EXTM    65      1000     full     yes    yes       up        EXTM
MGT1    66      1000     full      no     no       up        MGT1
```

The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex system chassis that you are using and the firmware versions and options that are installed.

Use this command to display link status information about each port on the CN4093, including:

- Port alias and port number
- 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 name

Port Information

The following command displays port information:

```
show interface information
```

Command mode: All

```
Alias   Port Tag RMON Lrn Fld PVID       NAME                 VLAN(s)
------- ---- --- ---- --- --- ----- -------------- --------------------------------
INTA1   1     n   d    e   e     1  INTA1          1
INTA2   2     n   d    e   e     1  INTA2          1
INTA3   3     n   d    e   e     1  INTA3          1
INTA4   4     n   d    e   e     2  INTA4          2
INTA5   5     n   d    e   e     1  INTA5          1
INTA6   6     n   d    e   e     1  INTA6          1
INTA7   7     n   d    e   e     1  INTA7          1
INTA8   8     n   d    e   e     1  INTA8          1
INTA9   9     n   d    e   e     1  INTA9          1
INTA10  10    n   d    e   e     1  INTA10         1
INTA11  11    n   d    e   e     1  INTA11         1
INTA12  12    n   d    e   e     1  INTA12         1
INTA13  13    n   d    e   e     1  INTA13         1
INTA14  14    n   d    e   e     1  INTA14         1
INTB1   15    n   d    e   e     1  INTB1          1
INTB2   16    n   d    e   e     1  INTB2          1
...
INTC13  41    n   d    e   e     1  INTC13         1
INTC14  42    n   d    e   e     1  INTC14         1
EXT1    43    n   d    e   e     1  EXT1           1
EXT2    44    n   d    e   e     1  EXT2           1
EXT3    45    n   d    e   e   100  EXT3           100
EXT4    46    n   d    e   e     1  EXT4           1
...
EXT20   62    n   d    e   e     1  EXT20          1
EXT21   63    n   d    e   e     1  EXT21          1
EXT22   64    n   d    e   e     1  EXT22          1
EXTM    65    n   d    e   e  4095  EXTM           4095
MGT1    66    y   d    e   e  4095  MGT1           4095

* = PVID is tagged.
```

The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis that you are using and the firmware versions and options that are installed.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Type of port (Internal, External, or Management)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB Learning enabled (`Lrn`)
- Whether the port has Port Flooding enabled (`Fld`)
- Port VLAN ID (PVID)
- Port name
- VLAN membership

Port Transceiver Status

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

```
show interface transceiver
```

Command mode: All

```
Name             TX  Link  TXFlt Volts DegsC TXuW  RXuW  Media   Laser  Approval
---------------- --- ----- ----- ----- ----- ----- ----- ------- ------ --------
44 SFP+  2       < NO Device Installed >
45 SFP+  3       Ena LINK  no     3.29 29.5  556.9 580.5 SR SFP+ 850nm  Approved
         Blade Network    Part:BN-CKM-SP-SR     Date:110329 S/N:AA1113AG1B1
46 SFP+  4       < NO Device Installed >
47 SFP+  5       N/A LINK  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:080710 S/N:BNT0828075
48 SFP+  6       < NO Device Installed >
49 SFP+  7       N/A Down  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:080710 S/N:BNT08280W0
50 SFP+  8       < NO Device Installed >
51 SFP+  9       N/A Down  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:100717 S/N:BNT10288NM
52 SFP+ 10       < NO Device Installed >
...
57 Q10G 15.1     < NO Device Installed >
58 Q10G 15.2     < NO Device Installed >
59 Q10G 15.3     < NO Device Installed >
60 Q10G 15.4     < NO Device Installed >
61 Q10G 16.1     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
62 Q10G 16.2     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
63 Q10G 16.3     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
64 Q10G 16.4     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
```

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

- Port number and media type
- TX: Transmission status
- 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 type (LX, LR, SX, SR)
- Laser wavelength, in nano-meters
- Approval status

The optical power levels shown for transmit and receive functions for the transceiver should fall within the expected range defined in the IEEE 802-3-2008 specification for each transceiver type. For convenience, the expected range values are summarized in the following table.

Table 65. Expected Transceiver Optical Power Levels

Transceiver Type	Tx Minimum	Tx Maximum	Rx Minimum	Rx Maximum
SFP SX	112μW	1000μW	20μW	1000μW
SFP LX	70.8μW	501μW	12.6μW	501μW
SFP+ SR	186μW	794μW	102μW	794μW
SFP+ LR	151μW	891μW	27.5μW	891μW

Note: Power level values in the IEEE specification are shown in dBm, but have been converted to mW in this table to match the unit of measure shown in the display output.

Virtual Machines Information

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

Table 66. 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 [-v]` Displays all Virtual Machine information. The -v option enables verbose mode. **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)
---------------- -----------------   ----- ------- ------------------
*127.31.46.50    00:50:56:4e:62:f5   4     INT3
*127.31.46.10    00:50:56:4f:f2:85   2     INT4
+127.31.46.51    00:50:56:72:ec:86   1     INT3
+127.31.46.11    00:50:56:7c:1c:ca   3     INT4
 127.31.46.25    00:50:56:9c:00:c8   5     INT4
 127.31.46.15    00:50:56:9c:21:2f   0     INT4
 127.31.46.35    00:50:56:9c:29:29   6     INT3

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
- Internal port on which the VM was detected
- VM group that contains the VM, if applicable

VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

Command mode: All

```
Default actions  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: the maximum number of acls
configurable on the switch (256)
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 67. 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 list of 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 68. 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  Type    MACAddress          Link
--------  ---------  ------  ------------  ------- ------------------  ---------
INTA1.1    1            101            25   Default  00:00:c9:5b:b7:d0   up
INTA2.2    2            102            10   Default  00:00:c9:5b:cf:d1   down
INTB1.2   12            202            25   Default  00:00:c9:5b:b7:c9   up
INTB9.4    #              *            25   Default           none       disabled

# = 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         : 101
Failover     : disabled

vNIC        Link
----------  ---------
INTA9.1     up
INTA10.1    up
INTB10.2    down

Port        Link
----------  ---------
INTA11    up

UplinkPort  Link
----------  ---------
EXT6        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)

SLP Information

The following commands display information about Service Location Protocol settings:

Table 69. SLP Information Options

Command Syntax and Usage
`show ip slp information` Displays the SLP version, whether SLP is enabled or disabled and whether DA auto-discovery is enabled or disabled **Command mode**: All
`show ip slp directory-agents` Lists all detected DAs **Command mode**: All
`show ip slp user-agents` Lists all detected UAs **Command mode**: All

Converged Enhanced Ethernet Information

Table 70 describes the Converged Enhanced Ethernet (CEE) information options.

Table 70. CEE Information Options

Command Syntax and Usage
`show cee information` Displays all CEE information, including DCBX, ETS and PFC. **Command mode:** All

DCBX Information

Table 71 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 71. 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 selected port. For details, see page 108. **Command mode:** All
`show cee information dcbx port <port alias or number> feature` Displays information about the DCBX Feature state machine for the selected port. For details, see page 109. **Command mode:** All
`show cee information dcbx port <port alias or number> ets` Displays information about the DCBX ETS state machine. For details, see page 110. **Command mode:** All
`show cee information dcbx port <port alias or number> pfc` Displays information about the DCBX PFC state machine. For details, see page 111. **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 selected port. For details, see page 111. **Command mode:** All
`show cee information dcbx port <port alias or number>` Displays all DCBX information. **Command mode:** All

DCBX Control Information

The following command displays DCBX Control information:

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

Command mode: All

```
Alias Port OperStatus OperVer MaxVer SeqNo AckNo
----- ---- ---------- ------- ------ ----- -----
INTA1 1     enabled    0       0      0     0
INTA2 2     enabled    0       0      4     2
INTA3 3     enabled    0       0      0     0
INTA4 4     enabled    0       0      1     1
...
```

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 or number*> `feature`

Command mode: All

```
DCBX Port Feature State-machine Info
====================================
Alias  Port Type    AdmState Will Advrt OpVer MxVer PrWill SeqNo Err OperMode Syncd
-----  ---- ------- -------- ---- ----- ----- ----- ------ ----- --- -------- ---
INTA1  1    ETS     enabled  No   Yes   0     0     No     0     No  disabled No
INTA2  2    ETS     enabled  No   Yes   0     0     Yes    4     No  enabled  Yes
INTA3  3    ETS     enabled  No   Yes   0     0     No     0     No  disabled No
INTA4  4    ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA5  5    ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA6  6    ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA7  7    ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA8  8    ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA9  9    ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA10 10   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
...
```

The following table describes the DCBX Feature information.

Table 72. 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

Table 72. DCBX Feature Information Fields

Parameter	Description
Err	Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange od 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
-----  ---- -------- ------- -------- --------
INTA2  2    0        PGID0   PGID0    PGID0
INTA2  2    1        PGID0   PGID0    PGID0
INTA2  2    2        PGID0   PGID0    PGID0
INTA2  2    3        PGID1   PGID0    PGID0
INTA2  2    4        PGID2   PGID0    PGID0
INTA2  2    5        PGID2   PGID0    PGID0
INTA2  2    6        PGID2   PGID0    PGID0
INTA2  2    7        PGID2   PGID0    PGID0

DCBX Port Priority Group - Bandwidth Allocation Table
=====================================================
Alias  Port PrioGrp BwDes BwOper BwPeer
-----  ---- ------- ----- ------ ------
INTA2  2    0       10    10     50
INTA2  2    1       50    50     50
INTA2  2    2       40    40     0
```

The following table describes the DCBX ETS information.

Table 73. 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
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 73. DCBX Feature Information Fields

Parameter	Description
DCBX Port Priority Group - Bandwidth Allocation Table	
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
----- ---- -------- ---------- ---------- ----------
INT2  2    0        disabled   disabled   disabled
INT2  2    1        disabled   disabled   disabled
INT2  2    2        disabled   disabled   disabled
INT2  2    3        enabled    disabled   disabled
INT2  2    4        disabled   disabled   disabled
INT2  2    5        disabled   disabled   disabled
INT2  2    6        disabled   disabled   disabled
INT2  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
----- ---- -------- ---------- ---------- ----------
INT2  2    0        enabled    enabled    enabled
INT2  2    1        disabled   disabled   disabled
INT2  2    2        disabled   disabled   disabled
INT2  2    3        enabled    enabled    enabled
INT2  2    4        disabled   disabled   disabled
INT2  2    5        disabled   disabled   disabled
INT2  2    6        disabled   disabled   disabled
INT2  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
----- ---- -------- ---------- ---------- ----------
INT2  2    0        enabled    enabled    enabled
INT2  2    1        disabled   disabled   disabled
INT2  2    2        disabled   disabled   disabled
INT2  2    3        enabled    enabled    enabled
INT2  2    4        disabled   disabled   disabled
INT2  2    5        disabled   disabled   disabled
INT2  2    6        disabled   disabled   disabled
INT2  2    7        disabled   disabled   disabled
```

The following table describes the DCBX Application Protocol information.

Table 74. 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

Table 74. DCBX Application Protocol Information Fields

Parameter	Description
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

ETS Information

Table 75 describes the Enhanced Transmission Selection (ETS) information options

Table 75. 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 76 describes the Priority Flow Control (PFC) information options.

Table 76. PFC Information Options

Command Syntax and Usage
`show cee port <port alias or number> pfc information` Displays PFC information.

The following command displays PFC information for a port:

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

Command mode: All

```
Global PFC Information:

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 Information

Table 77 describes the Fibre Channel over Ethernet (FCoE) information options.

Table 77. FCoE Information Options

Command Syntax and Usage
`show fcoe information` Displays all current FCoE information. **Command mode:** All

FIP Snooping Information

Table 78 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options

Table 78. FIP Snooping Information Options

Command Syntax and Usage
`show fcoe fips port` *<port alias or number>* `information` Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs. **Command mode:** All
`show fcoe fips fcf` Displays FCF information for all ports. **Command mode:** All
`show fcoe fips fcoe` Displays FCoE connections established on the switch. **Command mode:** All
`show fcoe fips information` Displays FIP Snooping information for all ports. **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.
```

FIP Snooping port information includes the following:

- Fiber Channel Forwarding (FCF) mode
- Number of FCF links connected to the port

- List of FIP Snooping ACLs assigned to the port

The following command displays Fibre Channel Forwarding FIP Snooping information:

`show fcoe fips fcf`

Command mode: All

```
Total number of FCFs detected: 10

     FCF MAC         Port    Vlan
-----------------------------------
08:17:f4:fb:c0:02    53      1004
08:17:f4:fb:c0:03    54      1004
08:17:f4:fb:c0:04    55      1002
08:17:f4:fb:c0:05    56      1003
...
08:17:f4:fb:c0:0d    64      1002
```

Fibre Channel Information

These commands allow you to display Fibre Channel information.

Table 79. Fibre Channel Information Commands

Command Syntax and Usage
`show flogi database` Displays fabric login database information. For details, see page 118. **Command mode:** All
`show fcalias` Displays the current FC alias - PWWN (port World Wide Name) mapping. **Command mode:** All
`show fcdomain` Displays the current configuration of FC domains. **Command mode:** All
`show fcns database` Displays FC name server database information. For details, see page 118. **Command mode:** All
`show fdmi database` Displays fibre channel management interface database information. **Command mode:** All
`show fcs database` Displays fabric configuration status database information. For details, see page 118. **Command mode:** All

Table 79. Fibre Channel Information Commands

Command Syntax and Usage
`show fcoe database` Displays Fibre Channel over Ethernet database information. **Command mode:** All
`show fcf` Displays Fibre Channel forwarding information. For details, see page 119. **Command mode:** All
`show npv status` Displays N_Port Virtualization information. **Command mode:** All
`show npv flogi-table` Displays the contents of the NPV fabric login table. **Command mode:** All
`show npv traffic-map` Displays NPV source-destination traffic mapping. For details, see page 119. **Command mode:** All
`show zone` Lists all FC zones. **Command mode:** All
`show zone status` Displays FC zone status information. For details, see page 119. **Command mode:** All
`show zone name` *<zone name>* Displays information for the specified FC zone. **Command mode:** All
`show zoneset` Lists all FC zonesets. **Command mode:** All
`show zoneset name` *<zoneset name>* Displays information for the specified FC zoneset. **Command mode:** All
`show zoneset active` Displays the currently active FC zoneset. **Command mode:** All

Table 79. Fibre Channel Information Commands

Command Syntax and Usage
`show interface fc information` Displays FC port information. For details, see page 120. **Command mode:** All
`show interface fc port` *<port no.>* Displays FC information for the specified ports. **Command mode:** All

Fabric Login Database Information

The following command displays a list of the storage devices present in the FC fabric login database:

```
show flogi database
```

Command mode: All

```
-------------------------------------------------------------------------
  Port   FCID            Port-WWN              Node-WWN
-------------------------------------------------------------------------
  EXT1  010c00     20:00:00:11:0d:64:f5:00    20:00:00:11:0d:64:f5:00
  EXT2  010c01     20:01:00:11:0d:64:f4:00    20:01:00:11:0d:64:f4:00

 Total number of entries = 2
```

Fibre Channel Name Server Database Information

The following command displays information about the FC name server database:

```
show fcns database
```

Command mode: All

```
-----------------------------------------
  FCID     TYPE  PWWN
-----------------------------------------
  010100   N    20:02:00:11:0d:8a:10:00
  010400   N    20:3a:00:80:e5:2d:1a:30
  010c00   N    10:00:00:00:27:1a:13:f0
  010c01   N    10:00:00:00:27:1a:13:f7
  010c02   N    10:00:00:00:27:1f:61:5d
  010c03   N    10:00:00:00:27:1f:61:3f
  010c04   N    10:00:00:00:27:1f:61:44
  010c05   N    10:00:00:00:27:1f:61:34
  010c06   N    10:00:00:00:27:1f:61:23
  010c07   N    10:00:00:00:27:1f:8e:18
...
  01140d   N    10:00:00:00:27:1f:61:4a

 Total number of entries = 72
```

Fabric Configuration Status Database Information

The following command displays information about the fabric configuration:

```
show fcs database
```

Command mode: All

```
Fabric Name        : 10:00:74:99:75:22:48:00
Switch Domain Id   : 1
Switch Mgmt Id     : 010000
Switch WWN         : 10:00:74:99:75:22:48:00
Switch Ports:
--------------------------------------------
Port        PWWN
--------------------------------------------
55    20:02:74:99:75:22:48:00
63    00:00:00:00:00:00:00:00
64    00:00:00:00:00:00:00:00
```

Fibre Channel Forwarding Information

The following command displays information about Fibre Channel forwarding:

```
show fcf
```

Command mode: All

```
==================================================
FCF:1 in VLAN: 1002    NPV-Gw
 FC-MAP      : 0x0efc00
 Priority    : 128
 FKA-Adv     : 8

 FC Port     : 55 60 63 64
==================================================
FCF:2 in VLAN: 1003    NPV-Gw
 FC-MAP      : 0x0efc01
 Priority    : 128
 FKA-Adv     : 8

 FC Port     : 56 59
==================================================
FCF:3 in VLAN: 1004    Fabric
 FC-MAP      : 0x0efc02
 Priority    : 128
 FKA-Adv     : 8

 FC Port     : 53 54 57 58 61 62
```

NPV Traffic Information

The following command displays information about NPV source-destination traffic mapping:

```
show npv traffic-mapping
```

Command mode: All

```
-------------------------------------------------------------------
 VLAN         Source Ports          NP-Uplink Dest Ports
-------------------------------------------------------------------
 1002                            55,60,63,64
 1003                            56,59
-------------------------------------------------------------------
```

Zone Status Information

The following command displays status information about FC zones:

```
show zone status
```

Command mode: All

```
Default-Zone           : Permit

FC Zoning Limits :--
MAX ZONES per ZONESET    :   64
MAX MEMBERS per ZONE     :   20

MAX ZONESETS             :    4
MAX ZONES                :  200
MAX ALIASES              :  200
MAX MEMBERS              : 1000
```

FC Port Information

The following command displays information about FC ports:

`show interface fc information`

Command mode: All

```
Alias   Port  Admin     Oper      Login        Config   Running  Link      Link
              State     State     Status       Type     Type     Status    Speed
-----   ----  -----     -----     ------       ------   -------  ------    -----
EXT11   53    Online    Online    LoggedIn     F        F        Active    4Gb/s
EXT12   54    Online    Offline   NotLoggedIn  F        F        Active    4Gb/s
EXT13   55    Online    Offline   NotLoggedIn  F        Unknown  Inactive  Unknown
EXT14   56    Online    Offline   NotLoggedIn  F        Unknown  Inactive  Unknown
EXT15   57    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT16   58    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT17   59    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT18   60    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT19   61    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT20   62    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT21   63    Down      Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
EXT22   64    Online    Downed    NotLoggedIn  Eth      Eth      Inactive  Unknown
```

Fibre Channel port information includes the following:

Table 80. Fibre Channel Port Information Descriptions

Parameter	Description
Alias	Port alias
Port	Port number
Admin State	Configured state of the port (`online`, `offline`, or `down`)
Oper State	Current operational state of the port (`online`, `offline`, or `downed`)
Login Status	Login status of the port on the FC fabric (`LoggedIn` or `NotLoggedIn`)
Config Type	Configured FC port type, as follows: – E (Expansion port) **not supported – F (Fabric port) – Eth (Ethernet port)

Table 80. Fibre Channel Port Information Descriptions (continued)

Parameter	Description
Running Type	Current operational FC port type, as follows: – E (Expansion port) **not supported – F (Fabric port) – Eth (Ethernet port) – Unknown
Link Status	Current status of the port link (`Active` or `Inactive`)
Link Speed	Current operational link speed.

The following command displays information specific FC ports:

`show interface fc port` <*port no.*>

Command mode: All

```
Port Number: EXT11
------------
AdminState                Online
ConfigType                F
EPortIsolationReason      NotApplicable
LinkSpeed                   Auto
LinkState                 Inactive
LoginStatus               NotLoggedIn
OperationalState          Offline
RunningType               Unkn
Port Number: EXT12
------------
AdminState                Online
ConfigType                F
EPortIsolationReason      NotApplicable
LinkSpeed                   Auto
LinkState                 Inactive
LoginStatus               NotLoggedIn
OperationalState          Offline
RunningType               Unkn
Port Number: EXT13
------------
AdminState                Online
ConfigType                Eth
EPortIsolationReason      NotApplicable
LinkSpeed                  10000
LinkState                 Inactive
LoginStatus               NotLoggedIn
OperationalState          Offline
RunningType               Eth
```

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 81. Statistics Commands

Command Syntax and Usage
`show layer3 counters` **Command mode:** All Displays Layer 3 statistics.
`show snmp-server counters` **Command mode:** All Displays SNMP statistics. See page 200 for sample output.
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. See page 204 for a sample output and a description of NTP Statistics. **Command mode:** All
`show ip slp counter` Displays Service Location Protocol packet counters. See page 205 for a sample output. **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. For details, see page 206. **Command mode:** All

Port Statistics

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

Table 82. Port Statistics Commands

Command Syntax and Usage
`show interface port <port alias or number> dot1x counters` Displays IEEE 802.1X statistics for the port. See page 125 for sample output. **Command mode:** All
`show interface port <port alias or number> bridging-counters` Displays bridging (“dot1”) statistics for the port. See page 128 for sample output. **Command mode:** All
`show interface port <port alias or number> ethernet-counters` Displays Ethernet (“dot3”) statistics for the port. See page 129 for sample output. **Command mode:** All
`show interface port <port alias or number> interface-counters` Displays interface statistics for the port. See page 132 for sample output. **Command mode:** All
`show interface port <port alias or number> ip-counters` Displays IP statistics for the port. See page 134 for sample output. **Command mode:** All
`show interface port <port alias or number> link-counters` Displays link statistics for the port. See page 135 for sample output. **Command mode:** All
`show interface port <port alias or number> rmon-counters` Displays Remote Monitoring (RMON) statistics for the port. See page 135 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

Table 82. Port Statistics Commands

Command Syntax and Usage
`clear interface port <port alias or number> counters` Clears all statistics for the port. **Command mode:** All except User EXEC
`clear counters` Clears statistics for all ports. **Command mode:** All except User EXEC

802.1X Authenticator Statistics

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

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

Command mode: All

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

Table 83. 802.1X Authenticator Statistics of a Port

Statistics	Description
eapolFramesRx	Total number of EAPOL frames received
eapolFramesTx	Total number of EAPOL frames transmitted
eapolStartFramesRx	Total number of EAPOL Start frames received
eapolLogoffFramesRx	Total number of EAPOL Logoff frames received
eapolRespIdFramesRx	Total number of EAPOL Response Identity frames received
eapolRespFramesRx	Total number of Response frames received
eapolReqIdFramesTx	Total number of Request Identity frames transmitted
eapolReqFramesTx	Total number of Request frames transmitted
invalidEapolFramesRx	Total number of invalid EAPOL frames received

Table 83. 802.1X Authenticator Statistics of a Port

Statistics	Description
eapLengthErrorFramesRx	Total number of EAP length error frames received
lastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
lastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

802.1X Authenticator Diagnostics

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

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

Command mode: All

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

Table 84. 802.1X Authenticator Diagnostics of a Port

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhile Connecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEntersAuthenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.

Table 84. 802.1X Authenticator Diagnostics of a Port

Statistics	Description
authSuccessesWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
authTimeoutsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.

Table 84. 802.1X Authenticator Diagnostics of a Port

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

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 INTA1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 85. 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.

Table 85. Bridging Statistics of a Port

Statistics	Description
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 INTA1:
dot3StatsAlignmentErrors:                  0
dot3StatsFCSErrors:                        0
dot3StatsSingleCollisionFrames:            0
dot3StatsMultipleCollisionFrames:          0
dot3StatsLateCollisions:                   0
dot3StatsExcessiveCollisions:              0
dot3StatsInternalMacTransmitErrors:       NA
dot3StatsFrameTooLongs:                    0
dot3StatsInternalMacReceiveErrors:         0
```

Table 86. Ethernet Statistics for 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.
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.
dot3StatsMultipleCollisionF rames	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.

Table 86. Ethernet Statistics for Port (continued)

Statistics	Description
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.
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 EXT1:
                     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

Ingress Discard reasons:                  Egress Discard reasons:

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

Table 87. Interface Statistics for 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.

Table 87. Interface Statistics for Port (continued)

Statistics	Description
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a 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.
VLAN Discards	Discarded because the packet was tagged with a VLAN to which this port is not a member.
Filter Discards	Dropped by the Content Aware Engine (user-configured filter).
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.

Table 87. Interface Statistics for Port (continued)

Statistics	Description
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	HOL-blocking Discards = Discarded because of Head Of Line (HOL) blocking mechanism. Low priority packets are placed in a separate queue and can be discarded as applications or the TCP protocol keep track of whether a retransmission is necessary or not. HOL blocking is necessary to wait until an overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of Memory Management Unit.
Other Discards	Discarded packets not included in any category.

Interface Protocol Statistics

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

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

Command mode: All

```
GEA IP statistics for port INTA1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 88. Interface Protocol Statistics

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

Link Statistics

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

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

Command mode: All

```
Link statistics for port INTA1:
linkStateChange:            1
```

Table 89. Link Statistics

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 90. 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.

Table 90. RMON Statistics of a Port (continued)

Statistics	Description
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.
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).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	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 90. RMON Statistics of a Port (continued)

Statistics	Description
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

QoS Queue Counter-Based Statistics

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

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

Command mode: All.

```
QoS statistics for port INTA14:
QoS Queue 0:
    Tx Packets:                          664872
    Dropped Packets:                          0
    Tx Bytes:                          46791050
    Dropped Bytes:                            0
QoS Queue 1:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 2:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 3:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 4:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 5:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 6:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 7:
    Tx Packets:                            9112
    Dropped Packets:                          0
    Tx Bytes:                            1463040
    Dropped Bytes:                            0
```

Table 91. QoS Queue Counter-Based Statistics of a Port

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

Table 91. QoS Queue Counter-Based Statistics of a Port (continued)

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

QoS Queue Rate-Based Statistics

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

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

Command mode: All.

```
QoS Rate for port INTA14:
QoS Queue 0:
    Tx Packets:                          5
    Dropped Packets:                     0
    Tx Bytes:                          363
    Dropped Bytes:                       0
QoS Queue 1:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 2:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 3:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 4:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 5:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 6:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
QoS Queue 7:
    Tx Packets:                          0
    Dropped Packets:                     0
    Tx Bytes:                            0
    Dropped Bytes:                       0
```

Table 92. QoS Queue Rate-Based Statistics of a Port

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

Trunk Group Statistics

Table 93. 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*> `counter` Clears all the statistics on the selected trunk group. **Command mode:** All except User EXEC

Layer 2 Statistics

Table 94. Layer 2 Statistics Commands

Command Syntax and Usage
`show mac-address-table counters` Displays FDB statistics. See page 143 for sample output. **Command mode:** All
`clear mac-address-table counters` Clears FDB statistics. **Command mode:** All except User EXEC
`show interface port` *<port alias or number>* `lacp counters` Displays Link Aggregation Control Protocol (LACP) statistics. See page 143 for sample output. **Command mode:** All
`clear interface port` *<port alias or number>* `lacp counters` Clears Link Aggregation Control Protocol (LACP) statistics. **Command mode:** All except User EXEC
`show hotlinks counters` Displays Hot Links statistics. See page 144 for sample output. **Command mode:** All except User EXEC
`clear hotlinks` Clears all Hot Links statistics. **Command mode:** All except User EXEC
`show interface port` *<port alias or number>* `lldp counters` Displays LLDP statistics. See page 145 for sample output. **Command mode:** All except User EXEC
`show oam counters` Displays OAM statistics. See page 146 for sample output. **Command mode:** All except User EXEC

FDB Statistics

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

```
show mac-address-table counters
```

Command mode: All

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

FDB statistics are described in the following table:

Table 95. 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 EXT1:
 -------------------------------------
 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 96. 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 96. LACP Statistics (continued)

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 97. 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 INTA1 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 98. 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 INTA1
----------------------------------------
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 99. vLAG Statistics Options

Command Syntax and Usage
`show vlag isl-statistics` Displays vLAG ISL statistics for the selected port. See page 147 for sample output.
`clear vlag statistics` Clears all vLAG statistics.
`show vlag statistics` Displays all vLAG statistics. See page 147 for sample output.

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:        0         System Info:           0
Peer Instance Enable: 0         Peer Instance Disable: 0
FDB Dynamic Add:      0         FDB Dynamic Del:       0
FDB Inactive Add:     0         FDB Inactive Del:      0
Health Check:         0         ISL Hello:             0
Other:                0         Unknown:               0

vLAG PDU received:
Role Election:        0         System Info:           0
Peer Instance Enable: 0         Peer Instance Disable: 0
FDB Dynamic Add:      0         FDB Dynamic Del:       0
FDB Inactive Add:     0         FDB Inactive Del:      0
Health Check:         0         ISL Hello:             0
Other:                0         Unknown:               0

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

The following table describes the vLAG statistics:

Table 100. 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.
Peer Instance Disable	Total number of vLAG PDUs sent for disabling peer instance.

Table 100. vLAG Statistics (continued)

Statistic	Description
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 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.
	vLAG IGMP packets forwarded
IGMP Reports	Total number of IGMP Reports forwarded over vLAG.
IGMP Leaves	Total number of IGMP Leave messages forwarded over vLAG.

Layer 3 Statistics

Table 101. Layer 3 Statistics Commands

Command Syntax and Usage
`show ip counters` Displays IP statistics. See page 152 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:** All except User EXEC
`show ip route counters` Displays route statistics. See page 160 for sample output. **Command mode:** All
`show ip arp counters` Displays Address Resolution Protocol (ARP) statistics. See page 161 for sample output. **Command mode:** All
`show ip dns counters` Displays Domain Name System (DNS) statistics. See page 161 for sample output. **Command mode:** All
`show ip icmp counters` Displays ICMP statistics. See page 162 for sample output. **Command mode:** All
`show ip tcp counters` Displays TCP statistics. See page 164 for sample output. **Command mode:** All
`show ip udp counters` Displays UDP statistics. See page 165 for sample output. **Command mode:** All
`show ip ospf counters` Displays OSPF statistics. See page 172 for sample output. **Command mode:** All
`show ipv6 ospf counters` Displays OSPFv3 statistics. See page 177 for sample output. **Command mode:** All

Table 101. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`show ip igmp counters` Displays IGMP statistics. See page 166 for sample output. **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 ipv6 mld counters` Displays Multicast Listener Discovery (MLD) statistics. See page 168 for more details and sample output. Command mode: All
`show ip vrrp counters` When virtual routers are configured, you can display the protocol statistics for VRRP. See page 181 for sample output. **Command mode:** All
`show ip pim counters` Displays PIM statistics for all configured PIM interfaces. See page 182 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*> `counters` Displays PIM statistics for the selected interface. **Command mode:** All
`show ip rip counters` Displays Routing Information Protocol (RIP) statistics. See page 183 for sample output. **Command mode:** All
`clear ip arp counters` Clears Address Resolution Protocol (ARP) statistics. **Command mode:** All except User EXEC

Table 101. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`clear ip dns counters` Clears Domain Name System (DNS) statistics. **Command mode:** All except User EXEC
`clear ip icmp counters` Clears Internet Control Message Protocol (ICMP) statistics. **Command mode:** All except User EXEC
`clear ip tcp counters` Clears Transmission Control Protocol (TCP) statistics. **Command mode:** All except User EXEC
`clear ip udp counters` Clears User Datagram Protocol (UDP) statistics. **Command mode:** All except User EXEC
`clear ip igmp` [<*VLAN number*>] `counters` Clears IGMP statistics. **Command mode:** All
`clear ip vrrp counters` Clears VRRP statistics. **Command mode:** All
`clear ip pim counters` Clears PIM statistics for all interfaces. **Command mode:** Privileged EXEC
`clear ip pim interface` <*interface 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:** All
`clear ip rip counters` Clears Routing Information Protocol (RIP) statistics. **Command mode:** All except User EXEC

Table 101. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`clear ip ospf counters` Clears Open Shortest Path First (OSPF) statistics. **Command mode:** All except User 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

Use the following command to clear IPv4 statistics:

```
clear ip counters
```

```
IP statistics:
ipInReceives:        3115873   ipInHdrErrors:           1
ipInAddrErrors:        35447   ipForwDatagrams:         0
ipInUnknownProtos:    500504   ipInDiscards:            0
ipInDelivers:        2334166   ipOutRequests:     1010542
ipOutDiscards:             4   ipOutNoRoutes:           4
ipReasmReqds:              0   ipReasmOKs:              0
ipReasmFails:              0   ipFragOKs:               0
ipFragFails:               0   ipFragCreates:           0
ipRoutingDiscards:         0   ipDefaultTTL:          255
ipReasmTimeout:            5
```

Table 102. IP Statistics

Statistic	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.

Table 102. IP Statistics (continued)

Statistic	Description
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.
ipForwDatagrams	The 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.
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).
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.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in `ipForwDatagrams`, which meet this *no-route* criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.

Table 102. IP Statistics (continued)

Statistic	Description
ipReasmFails	The 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.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The 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.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
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.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

IPv6 Statistics

The following command displays IPv6 statistics:

```
show ipv6 counters
```

Command mode: All

Use the following command to clear IPv6 statistics:

```
clear ipv6 counters
```

```
    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
```

Table 103 describes the IPv6 statistics.

Table 103. 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.
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.

Table 103. IPv6 Statistics (continued)

Statistic	Description
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).
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 104. 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.
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.

Table 104. ICMP Statistics (continued)

Statistic	Description
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 105 describes the UDP statistics.

Table 105. 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     :            1
Highest number ever recorded         :            1
Current static routes                :            0
Current RIP routes                   :            0
Current OSPF routes                  :            0
Current BGP routes                   :            0
Maximum supported routes             :         2048

ECMP statistics (active in ASIC):
--------------------------------
Maximum number of ECMP routes        :         2048
Maximum number of static ECMP routes :          128
Number of routes with ECMP paths     :            0
```

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
```

Table 106. 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.

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:          4095
```

Table 107. 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 108. 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 109. 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 109. ICMP Statistics

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
tcpCurBuff:              0   tcpCurConn:              3
tcpOutRsts:            417
```

Table 110. 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 110. TCP Statistics

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`).
tcpCurBuff	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 111. 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 Snoop 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
```

Table 112. 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 112. IGMP Statistics

Statistic	Description
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.
txIgmpGenQueries	Total number of General Membership Query packets transmitted.

MLD Statistics

Table 113 describes the commands used to view MLD statistics.

Table 113. MLD Statistics Commands

Command Syntax and Usage
`show ipv6 mld counters` Displays MLD statistics. See page 169 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 114. 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 115. OSPF Statistics Commands

Command Syntax and Usage
`show ip ospf counters` Displays OSPF statistics. **Command mode:** All See page 172 for sample output.
`show ip ospf area counters` Displays OSPF area statistics. **Command mode:** All except User EXEC
`show ip ospf interface` [<*interface number*>] `counters` Displays OSPF interface statistics. **Command mode:** All except User EXEC

OSPF Global Statistics

The following command displays statistics about OSPF packets received on all OSPF areas and interfaces:

```
show ip ospf counters
```

Command mode: All

```
OSPF stats
----------
Rx/Tx Stats:          Rx            Tx
                    --------      --------
  Pkts                 0             0
  hello               23           518
  database             4            12
  ls requests          3             1
  ls acks              7             7
  ls updates           9             7

Nbr change stats:                Intf change Stats:
  hello                  2            up                 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 116. 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 116. 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.

Table 116. OSPF General Statistics (continued)

Statistic	Description
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.
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.

Table 116. OSPF General Statistics (continued)

Statistic	Description
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:	
up	The sum total number of interfaces up in all OSPF 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 116. 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 117. OSPFv3 Statistics Commands

Command Syntax and Usage
`show ipv6 ospf counters` Displays OSPFv3 statistics. See page 172 for sample output. **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

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

Number of LSAs
  originated                      180
  rcvd newer originations         355
```

The OSPFv3 General Statistics contain the sum total of all OSPF packets received on all OSPFv3 areas and interfaces.

Table 118. 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.

Table 118. OSPFv3 General Statistics (continued)

Statistics		Description
	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.
Nbr Change Stats:		
	down	The total number of Neighboring routers down (that is, 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.

Table 118. OSPFv3 General Statistics (continued)

Statistics		Description
	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.

Table 118. OSPFv3 General Statistics (continued)

Statistics		Description
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.
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 CN4093 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
vrrpBadVersion:            0   vrrpBadVrid:              0
vrrpBadAddress:            0   vrrpBadData:              0
vrrpBadPassword:           0   vrrpBadInterval:          0
```

Table 119. 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.
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 120. 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
```

Management Processor Statistics

Table 121. Management Processor Statistics Commands

Command Syntax and Usage
`show mp thread` Displays STEM thread statistics. This command is used by Technical Support personnel. **Command mode:** All
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see page 185. **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 statistics, see page 193. **Command mode:** All
`show mp udp-block` Displays all UDP control blocks that are in use. To view a sample output, see page 194. **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 statistics, see page 194. **Command mode:** All
`show processes cpu history` Displays history of CPU utilization. To view a sample output, see page 195. **Command mode:** All

Packet Statistics

Table 122. 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 185. **Command mode:** All
`clear mp packet logs` Clears all CPU 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  0:13:36 Thu Mar 15, 2012

Packet rate:          Incoming            Outgoing
------------          --------            --------
1-second:                    5                   2
4-seconds:                   5                   1
64-seconds:                  5                   1

Packet counters:     Received                Sent
-----------------    --------                ----
Total packets:         359841              103895
Since bootup:          359841              103895

BPDUs:                  32240               32498
Cisco packets:              0                   0
ARP packets:           217226                   0
LACP packets:               0                   0
IPv4 packets:           88129               71397
 IGMP packets:              0                   0
 PIM packets:               0                   0
 ICMP Requests:             0               63586
 ICMP Replies:          63186                   0
 TCP  packets:              0                   0
  FTP                       0                   0
  HTTP                      0                   0
  SSH                       0                   0
  TACACS                    0                   0
  TELNET                    0                   0
  TCP other                 0                   0

 UDP packets:           28758                7811
  DHCP                  24872                7800
  NTP                      63                   0
  RADIUS                    0                   0
  SNMP                   3823                  11
  TFTP                      0                   0
  UDP other                63                   0
 RIP packets:               0                   0
 OSPF packets:              0                   0
 BGP packets:               0                   0
IPv6 packets:           22246                   0
LLDP PDUs:                  0                   0
ECP PDUs:                   0                   0
MgmtSock Packets:       63197               71397
Other:                      0                   0
...
```

```
 CPU packet statistics at  0:13:36 Thu Mar 15, 2012

Packet Buffer Statistics:
-------------------------
 allocs:        483682
 frees:         483681
 failures:           0
 dropped:            0

 small packet buffers:
 ----------------------
   current:                  0
   max:                   2048
   threshold:              512
   hi-watermark:             4
   hi-water time:    6:15:29 Wed Mar 14, 2012

 medium packet buffers:
 ----------------------
   current:                  1
   max:                   2048
   threshold:              512
   hi-watermark:             3
   hi-water time:    6:15:18 Wed Mar 14, 2012

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

 pkt_hdr statistics:
 ----------------------
 current          :           0
 max              :        3072
 hi-watermark     :           4
```

Statistics	Description
Packet rate	
1-second	The rate of incoming and outgoing packets over 1 second.
4-seconds	The rate of incoming and outgoing packets over 4 seconds.
64-seconds	The rate of incoming and outgoing packets over 64 seconds.
Packets counters	
Total packets	Total number of packets received and sent.
Since bootup	Total number of packets received and sent since the last switch reboot.

Statistics	Description
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received and sent.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received and sent.
ARP packets	Total number of Address Resolution Protocol packets received and sent.
IPv4 packets	Total number of IPv4 packets received and sent. Includes the following packet types: – IGMP – PIM – ICMP requests – ICMP replies
TCP packets	Total number of TCP packets received and sent. Includes the following packet types: – FTP – HTTP – SSH – TACACS+ – Telnet – Other
UDP packets	Total number of UDP packets received and sent. Includes the following packet types: – DHCP – NTP – RADIUS – SNMP – TFTP – Other
RIP packets	Total number of Routing Information Protocol packets received and sent.
OSPF packets	Total number of Open Shortest Path First packets received and sent.
BGP packets	Total number of Border Gateway Protocol packets received and sent.
IPv6 packets	Total number of IPv6 packets received and sent.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received and sent.
ECP PDUs	Total number of Edge Control Protocol data units received and sent.

Statistics	Description
MgmtSock Packets	Total number of packets received and transmitted through the management port.
Other	Total number of other packets received and transmitted.
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.
dropped	Total number of packets dropped by the packet buffer pool.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of medium packet allocations supported.
threshold	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.

Statistics	Description
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdr statistics	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack that are 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.

Packet Statistics Log

These commands allow you to display a log of all packets received by CPU. The following table describes the Packet Statistics Log options.

Table 123. Packet Statistics Log Options

Command Syntax and Usage
`show mp packet log all` Displays all packet logs received by and sent from the CPU. To view a sample output and a description of the log entries, see "Packet Log example" on page 190.
`show mp packet log rx` Displays all packets logs received by the CPU.
`show mp packet log tx` Displays all packet logs sent from the CPU.

Packet Log example

```
358. Type: BPDU, sent  1:01:11 Tue Mar 20, 2012
     Port EXT2, VLAN 201, Length 57, Reason 0x0, Flags 0x0
     Dst MAC: 01:80:c2:00:00:00, Src MAC: 08:17:f4:a7:57:2c

357. Type: ICMP ECHO Req,sent  1:01:09 Tue Mar 20, 2012
     Port MGT1, VLAN 4095, Length 16, Reason 0x0, Flags 0x0 FromMgmtSock
     Src IP: 9.43.98.125, Dst IP: 9.43.98.254
```

Each packet log entry includes the following information:

- Entry ID
- Packet type
- Date and time
- Port number
- VLAN number
- Packet length
- Reason code
- Flags
- Source and destination address

Packet Statistics Last Packet

These commands allow you to display a specified number (*N*) of the most recent packet logs received by or sent from the CPU. The following table describes the Packet Statistics Last Packet options.

Table 124. Last Packet Options

Command Syntax and Usage
`show mp packet last both` *<1-1000>* Displays a specified number of recent packet logs received by and sent from the CPU. To view a sample output and a description, see "Packet Log example" on page 190.
`show mp packet last rx` *<1-1000>* Displays a specified number of recent packet logs received by the CPU.
`show mp packet last tx` *<1-1000>* Displays a specified number of recent packet logs sent from the CPU.

Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

Table 125. Packet Statistics Dump Options

Command Syntax and Usage
`show mp packet dump all` Displays all packet statistics and logs received by and sent from the CPU.
`show mp packet dump rx` Displays all packet statistics and logs received by the CPU.

Table 125. Packet Statistics Dump Options

Command Syntax and Usage
`show mp packet dump tx` Displays all packet statistics and logs sent from the CPU.

Packet Statistics Parse

The following table describes the Packet Statistics Parse options.

Table 126. Packet Statistics Parse Options

Command Syntax and Usage
`show mp packet parse rx` <*packet type*> Displays specified packet types received by the CPU. Table 127 lists the packet types accepted by this command.
`show mp packet parse tx` <*packet type*> Displays specified packet types sent from the CPU. Table 127 lists the packet types accepted by this command.

Table 127. Packet types accepted by the packet parse command

Packet Type	Description
arp	Display only ARP packets logged.
bgp	Display only BGP packets logged.
bpdu	Display only BPDUs logged.
cisco	Display only Cisco packets (BPDU/CDP/UDLD) logged.
dhcp	Display only DHCP packets logged.
ecp	Display only ECP packets logged.
fcoe	Display only FCoE FIP PDUs logged.
ftp	Display only FTP packet logged.
http	Display only HTTP packets logged.
icmp	Display only ICMP packets logged.
igmp	Display only IGMP packet logged.
ip-addr	Display only logged packets with specified IP address.
ipv4	Display only IPv4 packets logged.
ipv6	Display only IPv6 packets logged.
lacp	Display only LACP packets logged.
lldp	Display only LLDP PDUs logged.
mac	Display only logged packets with specified MAC address.
mgmtsock	Display only packets logged from management ports.

Packet Type	Description
ntp	Display only NTP packets logged.
ospf	Display only OSPF packet logged.
other	Display logs of all packets not explicitly selectable.
pim	Display only PIM packet logged.
port	Display only logged packets with specified port.
radius	Display only RADIUS packets logged.
rarp	Display only Reverse-ARP packets logged.
raw	Display raw packet buffer in addition to headers.
rip	Display only RIP packet logged.
snmp	Display only SNMP packets logged.
ssh	Display only SSH packets logged.
tacacs	Display only TACACS packets logged.
tcp	Display only TCP packets logged.
tcpother	Display only TCP other-port packets logged.
telnet	Display only TELNET packets logged.
tftp	Display only TFTP packets logged.
udp	Display only UDP packets logged.
udpother	Display only UDP other-port packets logged.
vlan	Display only logged packets with specified VLAN.

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

```
Data Ports:
------------------------------------------------------------------
All TCP allocated control blocks:
1550c2c8:  0.0.0.0                                    0 <=>
           10.43.95.162                             443 listen MGT1 up
154c0f90:  0:0:0:0:0:0:0:0                            0 <=>
           0:0:0:0:0:0:0:0                          443  listen
154c1c98:  0.0.0.0                                    0 <=>
           0.0.0.0                                  443  listen
154c3d80:  0.0.0.0                                    0 <=>
...
Mgmt Ports:
------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.43.95.162:http       *:*                     LISTEN
tcp        0      0 10.43.96.33:http        *:*                     LISTEN
tcp        0      0 10.43.95.162:ssh        *:*                     LISTEN
...
```

Table 128. MP Specified TCP Statistics

Statistics	Description
1550c2c8	Memory
0.0.0.0	Destination IP address
0	Destination port
0.0.0.0/10.43.95.162	Source IP
443	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
  546:  listen


Mgmt Ports:
------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 9.43.95.121:snmp        *:*


0.0.0.0             0 <=> 9.43.95.121       161  accept  MGT1  up
```

CPU Statistics

The following command displays the CPU utilization statistics:

```
show mp cpu
```

Command mode: All .

```
       CPU utilization           Highest     Thread               Time
------------------------------   -------   ----------    -------------------------
cpuUtil1Second:            13%      93%    110 (FTMR)    11:36:19 Mon Jan 10, 2012
cpuUtil4Seconds:            7%
cpuUtil64Seconds:          13%
```

Table 129. CPU Statistics (stats/mp/cpu)

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage, highest rate, thread, and time the highest utilization occurred.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.
Highest	The highest percent ever recorded of CPU utilization.

Table 129. CPU Statistics (stats/mp/cpu)

Statistics	Description
Thread	Thread ID and name of the thread which caused highest CPU utilization.
Time	Time stamp that indicates when the hi-water mark was reached.

`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 130. 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.

History of CPU Statistics

The following command displays CPU utilization history:

`show mp cpu history`

Command mode: All

```
CPU Utilization History
-----------------------------------------------
  4 (TND ) 100% at  16:00:27 Wed Dec 31, 2012
127 (DONE) 100% at   1:34:43 Wed Mar  7, 2012
 20 (EPI )  55% at   1:34:53 Wed Mar  7, 2012
110 (ETMR)  56% at   1:34:54 Wed Mar  7, 2012
110 (ETMR)  64% at   1:34:56 Wed Mar  7, 2012
110 (ETMR)  68% at   1:35:01 Wed Mar  7, 2012
 94 (PROX)  75% at   2:46:54 Wed Mar  7, 2012
 94 (PROX)  84% at   2:46:55 Wed Mar  7, 2012
 94 (PROX)  84% at   2:46:57 Wed Mar  7, 2012
```

Access Control List Statistics

The following commands display and change ACL statistics.

Table 131. 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
`clear access-control list {<ACL number>|all} counters` Clears ACL statistics. **Command mode:** Privileged EXEC
`clear access-control list6 {<ACL number>|all}` 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
`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

The following command 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
```

Fibre Channel over Ethernet Statistics

The following command displays Fibre Channel over Ethernet (FCoE) statistics:

```
show fcoe counters
```

Command mode: All

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

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

Table 132. 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 Fibre Channel over Ethernet (FCoE) statistics:

```
clear fcoe counters
```

Command mode: Privileged EXEC

ACL Meter Statistics

This option displays ACL meter statistics.

```
show access-control meter <meter number> counters
```

Command mode: All

```
Out of profile hits for Meter 1, Port EXT1: 0
Out of profile hits for Meter 2, Port EXT1: 0
```

SNMP Statistics

The following command displays SNMP statistics:

```
show snmp-server counters
```

Command mode: All

```
SNMP statistics:
snmpInPkts:             150097   snmpInBadVersions:              0
snmpInBadC'tyNames:          0   snmpInBadC'tyUses:              0
snmpInASNParseErrs:          0   snmpEnableAuthTraps:            0
snmpOutPkts:            150097   snmpInBadTypes:                 0
snmpInTooBigs:               0   snmpInNoSuchNames:              0
snmpInBadValues:             0   snmpInReadOnlys:                0
snmpInGenErrs:               0   snmpInTotalReqVars:        798464
snmpInTotalSetVars:       2731   snmpInGetRequests:          17593
snmpInGetNexts:         131389   snmpInSetRequests:            615
snmpInGetResponses:          0   snmpInTraps:                    0
snmpOutTooBigs:              0   snmpOutNoSuchNames:             1
snmpOutBadValues:            0   snmpOutReadOnlys:               0
snmpOutGenErrs:              1   snmpOutGetRequests:             0
snmpOutGetNexts:             0   snmpOutSetRequests:             0
snmpOutGetResponses:    150093   snmpOutTraps:                   4
snmpSilentDrops:             0   snmpProxyDrops:                 0
```

Table 133. 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 133. 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.
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`.

Table 133. SNMP Statistics (continued)

Statistic	Description
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.
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.

Table 133. SNMP Statistics (continued)

Statistic	Description
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 SNMPv2 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 Networking 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/secondary server.
        Last update time: 18:04:16 Tue Jan 13, 2012
        Current system time: 18:55:49 Tue Jan 13, 2012
```

Table 134. 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 134. NTP Statistics (continued)

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`

SLP Statistics

Table 135. SLP Statistics Commands

Command Syntax and Usage
`show ip slp counter` Displays SLP packet counters. **Command mode:** All
`clear ip slp counter` Clears SLP packet counters. **Command mode:** Privileged EXEC

Use the following command to display SLP packet counters:

```
show ip slp counter
```

Command mode: All

```
    SLP Send Counters:
        SLP DAAdvert            : 0
        SLP SrvRqst             : 0
        SLP SrvRply             : 0
        SLP SrvAck              : 0
        SLP AttrRqst            : 0
        SLP AttrRply            : 0
        SLP SrvTypeRqst         : 0
        SLP SrvReg              : 0
        SLP SrvDeReg            : 0
        SLP SrvTypeRply         : 0
        SLP SAAdvert            : 0
        SLP Unknown             : 0

    SLP Receive Counters:
        SLP DAAdvert            : 0
        SLP SrvRqst             : 0
        SLP SrvRply             : 0
        SLP SrvAck              : 0
        SLP AttrRqst            : 0
        SLP AttrRply            : 0
        SLP SrvTypeRqst         : 0
        SLP SrvReg              : 0
        SLP SrvDeReg            : 0
        SLP SrvTypeRply         : 0
        SLP SAAdvert            : 0
        SLP Dropped             : 0
            Incorect pkt/dest   : 0
            Scopes mismatch     : 0
            Others              : 0
```

Statistics Dump

The following command dumps switch statistics:

```
show counters
```

Use the dump command to dump all switch statistics (40K or more, depending on your configuration). This data can be used to tune or debug switch performance.

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

Chapter 4. Configuration Commands

This chapter discusses how to use the Command Line Interface (CLI) for making, viewing, and saving switch configuration changes. Many of the commands, although not new, display more or different information than in the previous version. Important differences are called out in the text.

Table 136. General Configuration Commands

Command Syntax and Usage
`show running-config` Dumps current configuration to a script file. For details, see page 422. **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 423. **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
`copy running-config {ftp|tftp|sftp} [data-port|extm-port|mgt-port]` Backs up current configuration to a file on the selected FTP/TFTP/SFTP server. Select a management port, or press **Enter** to use the default (management) port. **Command mode:** Privileged EXEC

Table 136. General Configuration Commands

Command Syntax and Usage
`copy {ftp|tftp|sftp} running-config [data-port|extm-port|mgt-port]` Restores current configuration from a FTP/TFTP/SFTP server. Select a management port, or press **Enter** to use the default (management) port. For details, see page 423. **Command mode:** Privileged EXEC
`copy {tftp|sftp} {ca-cert|host-key|host-cert}` 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 **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 CN4093 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:

```
Router# 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 "Selecting a Configuration Block" on page 440.

System Configuration

These commands provide configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

Table 137. System Configuration Commands

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 Saving 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 28 **Command mode:** All

Table 137. System Configuration Commands (continued)

Command Syntax and Usage
`system idle` *<0-60>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes. A value of 0 disables system idle timeout. **Command mode:** Global configuration
`system linkscan {fast|normal|slow}` Configures the link scan interval used to poll the status of ports. **Command mode:** Global configuration
`system notice` *<maximum 1024 character multi-line login notice> <'.' to end>* Displays 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 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
`show system` Displays the current system parameters. **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 138. Error Disable Configuration Commands

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. **Command mode:** Global configuration
`show errdisable` Displays the current system Error Disable configuration. **Command mode:** All

System Host Log Configuration

Table 139. Host Log Configuration Commands

Command Syntax and Usage
[no] `logging host` *<1-2>* `address` *<IPv4 address>* [`data-port`|`extm-port`|`mgt-port`] Sets the IPv4 address of the first or second syslog host. **Command mode:** Global configuration
[no] `logging host` *<1-2>* `address6` *<IPv6 address>* [`data-port`|`extm-port`|`mgt-port`] Sets the IPv6 address of the first or second syslog host. **Command mode:** Global configuration

Table 139. Host Log Configuration Commands

Command Syntax and Usage
`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 <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 for unsolicited messages. When enabled, if unsolicited messages occur while solicited output display is in progress, the unsolicited messages are buffered and then output separately from the solicited messages. The buffer can store up to 20 unsolicited messages, after which unsolicited messages are discarded. When disabled, unsolicited and solicited messages are logged together. The `level` parameter sets a minimum severity level (lower or equal numeric values) for unsolicited messages to be displayed asynchronously; `all` displays all unsolicited messages asynchronously, regardless of severity level.The default setting is 2. **Command mode:** Global configuration
`[no] logging console severity <0-7>` Sets the severity level of system log messages to display 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. **Command mode:** Global configuration

Table 139. Host Log Configuration Commands

Command Syntax and Usage
[no] logging buffer severity <*0-7*> Sets the severity level of system log messages that are written to flash buffer. The system saves only messages with the selected severity level and above. For example, if you set the buffer severity to 2, only messages with severity level of 1 and 2 are saved. **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
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 27. The reverse option displays the output in reverse order, from the newest entry to the oldest. **Command mode:** All

SSH Server Configuration

For the CN4093 10Gb Converged Scalable Switch, these commands enable Secure Shell access from any SSH client.

Table 140. SSH Server Configuration Commands

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

RADIUS Server Configuration

Table 141. RADIUS Server Configuration Commands

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
`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-server 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

Table 141. RADIUS Server Configuration Commands

Command Syntax and Usage
`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 142. TACACS+ Server Configuration Commands

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
[`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

Table 142. TACACS+ Server Configuration Commands

Command Syntax and Usage
`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
`[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 CN4093, 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

Table 142. TACACS+ Server Configuration Commands

Command Syntax and Usage
[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
[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 [restricted|no-truncate] 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.
[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
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 143. LDAP Server Configuration Commands

Command Syntax and Usage
[no] ldap-server primary-host <*IP address*> Sets the primary LDAP server address. **Command mode:** Global configuration
[no] ldap-server secondary-host <*IP address*> 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 CN4093, contact your Service and Support line. **Command mode:** Global configuration
ldap-server enable Enables the LDAP server. **Command mode:** Global configuration

Table 143. LDAP Server Configuration Commands

Command Syntax and Usage
`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 Client Configuration

These commands allow you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 144. NTP Client Configuration Commands

Command Syntax and Usage
[no] `ntp primary-server` <*IP address*> `[-m|-mgt|-e|-extm|-d|-data]` Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: internal management port (`mgt`), external management port (`extm`), or data port (`data`). **Command mode:** Global configuration
[no] `ntp secondary-server` <*IP address*> `[-m|-mgt|-e|-extm|-d|-data]` Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: internal management port (`mgt`), external management port (`extm`), or data port (`data`). **Command mode:** Global configuration
[no] `ntp ipv6 primary-server` <*IPv6 address*> `[-m|-mgt|-e|-extm|-d|-data]` Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: internal management port (`mgt`), external management port (`extm`), or data port (`data`). **Note**: To delete the IPv6 primary server, use the following command: `no ntp primary-server` <*IP address*> **Command mode:** Global configuration

Table 144. NTP Client Configuration Commands

Command Syntax and Usage
[no] ntp ipv6 secondary-server <*IPv6 address*> [-m|-mgt|-e|-extm|-d|-data] Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: internal management port (mgt), external management port (extm), or data port (data). **Note**: To delete the IPv6 secondary server, use the following command: no ntp secondary-server <*IP address*> **Command mode:** Global configuration
ntp interval <*5-44640*> Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server. **Command mode:** Global configuration
ntp source loopback <*1-5*> Sets the NTP source loopback interface. **Command mode:** Global configuration
[no] ntp authenticate Enables or disables NTP authentication. The default setting is disabled. When authentication is enabled, the switch transmits NTP packets with the MAC address appended. **Command mode:** Global configuration
ntp primary-key <*1-65534*> Adds the NTP primary server key, which specifies which MD5 key is used by the primary server. **Command mode:** Global configuration
ntp secondary-key <*1-65534*> Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server. **Command mode:** Global configuration
ntp trusted-key <*1-65534*>|0 Adds an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code. **Command mode:** Global configuration
ntp enable Enables the NTP synchronization service. **Command mode:** Global configuration

Table 144. NTP Client Configuration Commands

Command Syntax and Usage
`no ntp enable` Disables the NTP synchronization service. **Command mode:** Global configuration
`show ntp` Displays the current NTP service settings. **Command mode:** All

NTP MD5 Key Commands

Table 145. NTP MD5 KEy Configuration Options

Command Syntax and Usage
`ntp message-digest-key` <*1-65534*> `md5-key` <*1-16 characters*> Configures the selected MD5 key code. **Command mode:** Global configuration
`no ntp message-digest-key` <*1-65534*> Deletes the selected MD5 key code. **Command mode:** Global configuration

System SNMP Configuration

IBM Networking 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 146. System SNMP Commands

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

Table 146. System SNMP Commands

Command Syntax and Usage
`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 ports, 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 the sending of SNMP link up and link down traps. The default setting is `enabled`. **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 147. SNMPv3 Configuration Commands

Command Syntax and Usage
`snmp-server user <1-16>` 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 228.
`snmp-server view <1-128>` This command allows you to create different MIB views. **Command mode:** Global configuration To view command options, see page 229.
`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 230.
`snmp-server group <1-16>` 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 232.
`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 232.

Table 147. SNMPv3 Configuration Commands

`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 page 233.
`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 page 234.
`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 page 235.
`snmp-server version {v1v2v3|v3only}` This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. The default setting is `v3only`. **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 148. User Security Model Configuration Commands

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, or none. The default algorithm is `none`. 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|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) 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). 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
`no snmp-server user <1-16>` Deletes the USM user entries. **Command mode:** Global configuration
`show snmp-server v3 user <1-16>` 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 149. SNMPv3 View Configuration Commands

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 150. View-based Access Control Model Commands

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> prefix <1-32 characters>` Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by contextName. **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> match {exact|prefix}` If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected. **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

Table 150. View-based Access Control Model Commands

Command Syntax and Usage
`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 151. SNMPv3 Group Configuration Commands

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 228: `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 228. **Command mode:** Global configuration
`no snmp-server group <1-16>` Deletes the `vacmSecurityToGroup` entry. **Command mode:** Global configuration
`show snmp-server v3 group <1-16>` 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 152. SNMPv3 Community Table Configuration Commands

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 page 228: `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

Table 152. SNMPv3 Community Table Configuration Commands (continued)

Command Syntax and Usage
`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 153. Target Address Table Configuration Commands

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 address that can be used in the generation of SNMP traps. **Command mode:** Global configuration
`snmp-server target-address <1-16> port <port number>` 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 page 234: `snmp-server target-parameters <1-16> name <1-32 characters>` **Command mode:** Global configuration

Table 153. Target Address Table Configuration Commands (continued)

Command Syntax and Usage
`no snmp-server target-address <1-16>` Deletes the Target Address Table entry. **Command mode:** Global configuration
`show snmp-server v3 target-address <1-16>` Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

You can configure the target parameters entry and store it in the target parameters table in the SNMP engine. This table contains parameters that are used to generate a message. The parameters include the message processing model (for example: SNMPv3, SNMPv2c, SNMPv1), the security model (for example: USM), the security name, and the security level (`noAuthnoPriv`, `authNoPriv`, or `authPriv`).

Table 154. Target Parameters Table Configuration Commands

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

Table 154. Target Parameters Table Configuration Commands (continued)

Command Syntax and Usage
`snmp-server target-parameters <1-16> level {noAuthNoPriv|authNoPriv|authPriv}` Allows you to select the level of security to be used when generating the SNMP messages using this entry. 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 155. Notify Table Commands

Command Syntax and Usage
`snmp-server notify <1-16> name <1-32 characters>` Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry. **Command mode:** Global configuration
`snmp-server notify <1-16> tag <1-255 characters>` Allows you to configure a tag that contains a tag value which is used to select entries in the Target Address Table. Any entry in the `snmpTargetAddrTable`, that matches the value of this tag, is selected. **Command mode:** Global configuration
`no snmp-server notify <1-16>` Deletes the notify table entry. **Command mode:** Global configuration
`show snmp-server v3 notify <1-16>` Displays the current notify table configuration. **Command mode:** All

System Access Configuration

The following table describes system access configuration commands.

Table 156. System Access Configuration Commands

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 CN4093, 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 http enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. The default setting is `disabled`. **Command mode:** Global configuration
`[default] access http port [`<*port number*>`]` Sets the switch port used for serving switch Web content. The default is HTTP port 80. Command mode: Global configuration

Table 156. System Access Configuration Commands

Command Syntax and Usage
[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. The default setting is disabled. **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 157. Management Network Configuration Commands

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

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 158. User Access Control Configuration Commands

Command Syntax and Usage
`access user` *<1-10>* Configures the User ID. **Command mode:** Global configuration
`access user eject` {*<user name>*|*<session id>*} Ejects the specified user from the CN4093. **Command mode:** Global configuration

Table 158. User Access Control Configuration Commands

Command Syntax and Usage
`clear line <1-12>` Ejects the user with the corresponding session ID from the CN4093. **Command mode:** Privileged EXEC
`access user user-password <1-128 characters>` Sets the user (`user`) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes. **Command mode:** Global configuration
`access user operator-password <1-128 characters>` 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. **Command mode:** Global configuration
`access user administrator-password <1-128 characters>` Sets the administrator (`admin`) password. The super user administrator has complete access to all information and configuration commands on the CN4093, including the ability to change both the user and administrator passwords. Access includes "`oper`" functions. **Command mode:** Global configuration
`show access user` Displays the current user status. **Command mode:** All

System User ID Configuration

The following table describes user ID configuration commands.

Table 159. User ID Configuration Commands

Command Syntax and Usage
`access user <1-10> level {user|operator|administrator}` Sets the Class-of-Service to define the user's authority level. IBM Networking OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level. **Command mode:** Global configuration
`access user <1-10> name <1-8 characters>` Defines the user name of maximum eight characters. **Command mode:** Global configuration

Table 159. User ID Configuration Commands

Command Syntax and Usage
`access user <1-10> 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 <1-10> enable` Enables the user ID. **Command mode:** Global configuration
`no access user <1-10> enable` Disables the user ID. **Command mode:** Global configuration
`no access user <1-10>` Deletes the user ID. **Command mode:** Global configuration
`show access user` Displays the current user ID configuration. **Command mode:** All

Strong Password Configuration

The following table describes strong password configuration commands.

Table 160. Strong Password Configuration Commands

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

Table 160. Strong Password Configuration Commands

Command Syntax and Usage
`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

HTTPS Access Configuration

The following table describes HTTPS access configuration commands.

Table 161. HTTPS Access Configuration Commands

Command Syntax and Usage
`[no] access https enable` Enables or disables BBI access (Web access) using HTTPS. The default setting is `enabled`. **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): IBM – Organizational Unit Name (for example, section): Operations – Common Name (for example, user's name): Mr Smith – Email (for example, email address): info@ibm.com You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent. **Command mode:** Global configuration

Table 161. HTTPS Access Configuration Commands

Command Syntax and Usage
`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
`show access` Displays the current SSL Web Access configuration. **Command mode:** All

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 162. Custom DST Configuration Commands

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 calender 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 calender 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

Table 162. Custom DST Configuration Commands

Command Syntax and Usage
`system custom-dst enable` Enables the Custom Daylight Saving Time settings. **Command mode:** Global configuration
`no system custom-dst enable` Disables the Custom Daylight Savings Time settings. **Command mode:** Global configuration
`show custom-dst` Displays the current Custom DST configuration. **Command mode:** All

sFlow Configuration

IBM Networking 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 163. sFlow Configuration Commands

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>* Defines the sFlow server address. **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

Note: Use the following commands to configure the sFlow port on the switch.

Table 164. sFlow Port Configuration Commands

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` <*256-65536*> Configures the sFlow sampling rate, in packets per sample. The default setting is `disabled`. **Command mode:** Interface port

Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INT*x*) and (EXT*x*). If you are configuring management ports (MGT1 or EXTM), see "Management Port Configuration" on page 253.

Table 165. Port Configuration Commands

Command Syntax and Usage
`interface port` *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
`dot1p` *<0-7>* Configures the port's 802.1p priority level. **Command mode:** Interface port
`pvid` *<VLAN number>* Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports. **Command mode:** Interface port
`name` *<1-64 characters>* Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default is set to `None`. **Command mode:** Interface port
`[no] bpdu-guard` Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.
`[no] dscp-marking` Enables or disables DSCP re-marking on a port. **Command mode:** Interface port
`[no] rmon` Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function. **Command mode:** Interface port
`[no] tagging` Disables or enables VLAN tagging for this port. The default setting is `disabled` for external ports (EXT*x*) and `enabled` for internal server ports (INT*x*). **Command mode:** Interface port
`[no] tag-pvid` Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is `disabled` for internal server ports (INT*x*) and external ports (EXT*x*), and `enabled` for management (MGT*x*) ports. **Command mode:** Interface port

Table 165. Port Configuration Commands (continued)

Command Syntax and Usage
`[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
`port-channel min-links <1-16>` 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
`[no] broadcast-threshold <0-262143>` Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets. **Command mode:** Interface port
`[no] multicast-threshold <0-262143>` Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets. **Command mode:** Interface port
`[no] dest-lookup-threshold <0-262143>` Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets. **Command mode:** Interface port
`no shutdown` Enables the port. **Command mode:** Interface port
`shutdown` Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 248.) **Command mode:** Interface port
`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 166. Port Error Disable Commands

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

Port Link Configuration

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

Table 167. Port Link Configuration Commands

Command Syntax and Usage
`speed {10|100|1000|10000|auto}` Sets the link speed. Some options are not valid on all ports. The choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – 10000 Mps – any (auto negotiate port speed) **Command mode:** Interface port
`duplex {full|half|any}` Sets the operating mode. The choices include: – “Any,” for auto negotiation (default) – Half-duplex – Full-duplex **Command mode:** Interface port

Table 167. Port Link Configuration Commands

Command Syntax and Usage
`[no] flowcontrol {receive|send|both}` Sets the flow control. The choices include: – Receive flow control – Transmit flow control – Both receive and transmit flow control (default) – No flow control **Note**: For external ports (EXT*x*) the default setting is no flow control, and for internal ports (INT*x*) the default setting is both receive and transmit. **Command mode:** Interface port
`[no] auto` Turns auto-negotiation on or off.
`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:

```
Router# 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 CN4093 10Gb Converged Scalable Switch is reset. See the "Operations Commands" on page 425 for other operations-level commands.

UniDirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 168. Port UDLD Configuration Commands

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 alias or 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 169. Port OAM Configuration Commands

Command Syntax and Usage
`oam {active|passive}` Configures the OAM discovery mode, as follows: – Active: This port link initiates OAM discovery. – 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 {active|passive}` Disables OAM discovery on the port. **Command mode:** Interface port
`show oam` Displays current port OAM parameters. **Command mode:** All

Port ACL Configuration

The following table describes port ACL configuration commands

Table 170. Port ACL/QoS Configuration Commands

Command Syntax and Usage
`[no] access-control list` *<ACL number>* Adds or removes the specified ACL. You can add multiple ACLs to a port. **Command mode:** Interface port
`[no] access-control list6` *<ACL number>* Adds or removes the specified IPv6 ACL. You can add multiple ACLs to a port. **Command mode:** Interface port
`[no] access-control group` *<ACL group number>* Adds or removes the specified ACL group. You can add multiple ACL groups to a port. **Command mode:** Interface port
`show interface port` *<port alias or number>* `access-control` Displays current ACL QoS parameters. **Command mode:** All

Port Spanning Tree Configuration

Table 171. Port STP Commands

Command Syntax and Usage
`[no] spanning-tree edge` Enables or disables this port as an 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
`[no] spanning-tree link-type p2p|shared` Defines the type of link connected to the port, as follows: – `no`: 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
`show interface port {`*<port alias or number>*`}` Displays current port configuration parameters. **Command mode:** All

Port Spanning Tree Guard Configuration

Table 172. Port STP Guard Options

Command Syntax and Usage
`spanning-tree guard loop` Enables STP loop guard. STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received. **Command mode:** Interface port/Interface portchannel
`spanning-tree guard root` Enables STP root guard. STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening). **Command mode:** Interface port/Interface portchannel

Table 172. Port STP Guard Options

Command Syntax and Usage
`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

Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see "Weighted Random Early Detection Configuration" on page 258.

Table 173. Port WRED Options

Command Syntax and Usage
`[no] random-detect ecn enable` Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions. **Note**: ECN functions only on TCP traffic. **Command mode:** Interface port
`random-detect enable` Turns on Random Detection and avoidance. **Command mode:** Interface port
`no random-detect enable` Turns off Random Detection and avoidance. **Command mode:** Interface port
`show interface port` <*port alias or number*> `random-detect` Displays current Random Detection and avoidance parameters. **Command mode:** All

Port WRED Transmit Queue Configuration

Use this menu to define WRED thresholds for the port's transmit queues. Set each threshold between 1% and 100%. When the average queue size grows beyond the minimum threshold, packets begin to be dropped. When the average queue size reaches the maximum threshold, all packets are dropped. The probability of packet-drop between the thresholds is defined by the drop rate.

Table 174. Port WRED Transmit Queue Options

Command Syntax and Usage
`[no] random-detect transmit-queue` *<0-7>* `tcp` *<min. threshold (1-100)>* *<max. threshold (1-100)>* *<drop rate (1-100)>` Configures the WRED thresholds for TCP traffic. Use the `no` form to clear the WRED threshold value. **Command mode:** Interface port
`[no] random-detect transmit-queue` *<0-7>* `non-tcp` *<min. threshold (1-100)>* *<max. threshold (1-100)>* *<drop rate (1-100)>` Configures the WRED thresholds for non-TCP traffic. Use the `no` form to clear the WRED threshold value. **Command mode:** Interface port
`random-detect transmit-queue` *<0-7>* `enable` Sets the WRED transmit queue configuration to `on`. **Command mode:** Interface port
`no random-detect transmit-queue` *<0-7>* `enable` Sets the WRED transmit queue configuration to `off`. **Command mode:** Interface port

Management Port Configuration

You can use these commands to set port parameters for management ports (MGT1 and EXTM). Use these commands to set port parameters for the port link. For MGT1, the values for speed, duplex, and flow control are fixed, and cannot be configured.

Table 175. Management Port Configuration Commands

Command Syntax and Usage
`speed {10|100|1000|auto}` Sets the link speed. The choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – Auto — for auto negotiation **Command mode:** Interface port

Table 175. Management Port Configuration Commands (continued)

Command Syntax and Usage
`duplex {full|half|any}` Sets the operating mode. The choices include: – Full-duplex – Half-duplex – Any — for auto negotiation (default) **Command mode:** Interface port
`[no] flowcontrol {receive|send|both}` Sets the flow control. The choices include: – Receive flow control – Transmit flow control – Both receive and transmit flow control (default) – No flow control **Command mode:** Interface port
`no shutdown` Enables the port. **Command mode:** Interface port
`shutdown` Disables the port. **Command mode:** Interface port
`show interface port` <*port alias or number*> Displays current port 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 CN4093 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 176. 802.1p Configuration Commands

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 177. DSCP Configuration Commands

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

Table 177. DSCP Configuration Commands

Command Syntax and Usage
`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

Control Plane Protection

These commands allow you to limit the number of selected protocol packets received by the control plane (CP) of the switch. These limits help protect the CP from receiving too many protocol packets in a given time period.

Table 178. Control Plane Protection Options

Command Syntax and Usage
`qos protocol-packet-control packet-queue-map` *<packet queue number (0-40)> <packet type>* Configures a packet type to associate with each packet queue number. Enter a queue number, followed by the packet type. You may map multiple packet types to a single queue. The following packet types are allowed: – **802.1x** (IEEE 802.1x packets) – **application-cri-packets** (critical packets of various applications, such as Telnet, SSH) – **arp-bcast** (ARP broadcast packets) – **arp-ucast** (ARP unicast reply packets) – **bgp** (BGP packets) – **bpdu** (Spanning Tree Protocol packets) – **cisco-bpdu** (Cisco STP packets) – **dest-unknown** (packets with destination not yet learned) – **dhcp** (DHCP packets) – **icmp** (ICMP packets) – **igmp** (IGMP packets) – **ipv4-miscellaneous** (IPv4 packets with IP options and TTL exception) – **ipv6-nd** (IPv6 Neighbor Discovery packets) – **lacp** (LACP/Link Aggregation protocol packets) – **lldp** (LLDP packets) – **ospf** (OSPF packets) – **ospf3** (OSPF3 Packets) – **pim** (PIM packets) – **rip** (RIP packets) – **system** (system protocols, such as tftp, ftp, telnet, ssh) – **udld** (UDLD packets) – **vlag** (vLAG packets) – **vrrp** (VRRP packets) **Command mode:** Global configuration
`qos protocol-packet-control rate-limit-packet-queue` *<packet queue number (0-40)> <1-10000>* Configures the number of packets per second allowed for each packet queue. **Command mode:** Global configuration

Table 178. Control Plane Protection Options (continued)

Command Syntax and Usage
`no qos protocol-packet-control packet-queue-map` *<packet type>* Clears the selected packet type from its associated packet queue. **Command mode:** Global configuration
`no qos protocol-packet-control rate-limit-packet-queue` *<packet queue number (0-40)>* Clears the packet rate configured for the selected packet queue. **Command mode:** Global configuration
`show qos protocol-packet-control information protocol` Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. **Command mode:** All
`show qos protocol-packet-control information queue` Displays the packet rate configured for each packet queue. **Command mode:** All

Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. CN4093 implementation of WRED defines TCP and non-TCP traffic profiles on a per-port, per COS queue basis. For each port, you can define a transmit-queue profile with thresholds that define packet-drop probability.

These commands allow you to configure global WRED parameters. For port WRED commands, see "Port WRED Configuration" on page 252.

Table 179. WRED Configuration Options

Command Syntax and Usage
`qos random-detect ecn` Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions. **Note**: ECN functions only on TCP traffic. **Command mode:** Global configuration
`qos random-detect enable` Turns on Random Detection and avoidance. **Command mode:** Global configuration

Table 179. WRED Configuration Options

Command Syntax and Usage
`no qos random-detect enable` Turns off Random Detection and avoidance. **Command mode:** Global configuration
`show qos random-detect` Displays current Random Detection and avoidance parameters. **Command mode:** All

WRED Transmit Queue Configuration

Table 180. WRED Transmit Queue Options

Command Syntax and Usage
`[no] qos random-detect transmit-queue` *<0-7>* `tcp` *<min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>* Configures the WRED thresholds for TCP traffic. Use the `no` form to clear the WRED threshold value. **Command mode:** Global configuration
`[no] qos random-detect transmit-queue` *<0-7>* `non-tcp` *<min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)>* Configures the WRED thresholds for non-TCP traffic. Use the `no` form to clear the WRED threshold value. **Command mode:** Global configuration
`qos random-detect transmit-queue` *<0-7>* `enable` Sets the WRED transmit queue configuration to `on`. **Command mode:** Global configuration
`no qos random-detect transmit-queue` *<0-7>* `enable` Sets the WRED transmit queue configuration to `off`. **Command mode:** Global configuration

Access Control Configuration

Use these commands to create Access Control Lists and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

For information about assigning ACLs to ports, see “Port ACL Configuration” on page 250.

Table 181. General ACL Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> Configures an Access Control List. **Command mode:** Global configuration To view command options, see page 261.
[no] access-control group <*1-256*> Configures an ACL Group. **Command mode:** Global configuration To view command options, see page 270.
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 182. ACL Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> egress-port port <*port alias or number*> Configures the ACL to function on egress packets. **Command mode:** Global configuration
access-control list <*1-256*> action {permit|deny|set-priority <*0-7*>} Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
[no] access-control list <*1-256*> statistics Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration
default access-control list <*1-256*> Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list <*1-256*> Displays the current ACL parameters. **Command mode:** All
[no] access-control list6 <*1-128*> Configures an IPv6 Access Control List. To view command options, see page 265. **Command mode:** Global configuration

Ethernet Filtering Configuration

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

Table 183. Ethernet Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> ethernet source-mac-address <*MAC address*> <*MAC mask*> Defines the source MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> ethernet destination-mac-address <*MAC address*> <*MAC mask*> Defines the destination MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> ethernet vlan <*VLAN ID*> <*VLAN mask*> Defines a VLAN number and mask for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> ethernet ethernet-type {arp|ip|ipv6|mpls|rarp|any|<*other (0x600-0xFFFF)*>} Defines the Ethernet type for this ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> ethernet priority <*0-7*> Defines the Ethernet priority value for the ACL. **Command mode:** Global configuration
default access-control list <*1-256*> ethernet Resets Ethernet parameters for the ACL to their default values. **Command mode:** Global configuration
no access-control list <*1-256*> ethernet Removes Ethernet parameters for the ACL. **Command mode:** Global configuration
show access-control list <*1-256*> ethernet Displays the current Ethernet parameters for the ACL. **Command mode:** All

IPv4 Filtering Configuration

These commands allow you to define IPv4 matching criteria for an ACL.

Table 184. IP version 4 Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> ipv4 source-ip-address <*IP address*> <*IP mask*> Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation. **Command mode:** Global configuration
[no] access-control list <*1-256*> ipv4 destination-ip-address <*IP address*> <*IP mask*> Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> ipv4 protocol <*0-255*> Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp **Command mode:** Global configuration
[no] access-control list <*1-256*> ipv4 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 <*1-256*> ipv4 Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-256*> ipv4 Displays the current IPv4 parameters. **Command mode:** All

TCP/UDP Filtering Configuration

These commands allow you to define TCP/UDP matching criteria for an ACL.

Table 185. TCP/UDP Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> tcp-udp source-port <*1-65535*> *<mask (0xFFFF)>* Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports: **Number Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
[no] access-control list <*1-256*> tcp-udp destination-port <*1-65535*> *<mask (0xFFFF)>* Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with sport above. **Command mode:** Global configuration
[no] access-control list <*1-256*> tcp-udp flags *<value (0x0-0x3f)> <mask (0x0-0x3f)>* Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
default access-control list <*1-256*> tcp-udp Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-256*> tcp-udp Displays the current TCP/UDP Filtering parameters. **Command mode:** All

Packet Format Filtering Configuration

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

Table 186. Packet Format Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-256*> packet-format ethernet {ethertype2| snap|llc} Defines the Ethernet format for the ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> packet-format tagging {any|none|tagged} Defines the tagging format for the ACL. **Command mode:** Global configuration
[no] access-control list <*1-256*> packet-format ip {ipv4|ipv6} Defines the IP format for the ACL. **Command mode:** Global configuration
default access-control list <*1-256*> packet-format Resets Packet Format parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-256*> packet-format Displays the current Packet Format parameters for the ACL. **Command mode:** All

ACL IPv6 Configuration

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

Table 187. IPv6 ACL Options

Command Syntax and Usage
[no] access-control list6 <*1-128*> egress-port port <*port alias or number*> Configures the ACL to function on egress packets. **Command mode:** Global configuration
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

Table 187. IPv6 ACL Options

Command Syntax and Usage
`default access-control list6 <1-128>` Resets the ACL parameters to their default values. **Command mode:** Global configuration
`show access-control list <1-128>` Displays the current ACL parameters. **Command mode:** All

IPv6 Filtering Configuration

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

Table 188. 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.
[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.
[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.
`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 189. 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 190. 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
`[no] access-control list6 <1-128> re-mark use-tos-precedence` Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`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

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 261.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration" on page 309.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 414.

Table 191 lists the general VMAP configuration commands.

Table 191. VMAP Configuration Commands

Command Syntax and Usage
[no] access-control vmap <*1-128*> egress-port <*port alias or number*> Configures the VMAP to function on egress packets. **Command mode:** Global configuration
access-control vmap <*1-128*> action {permit|deny| set-priority <*0-7*>} Configures a filter action for packets that match the VMAP definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
[no] access-control vmap <*1-128*> statistics Enables or disables the statistics collection for the VMAP. **Command mode:** Global configuration
default access-control vmap <*1-128*> Resets the VMAP parameters to their default values. **Command mode:** Global configuration
show access-control vmap <*1-128*> Displays the current VMAP parameters. **Command mode:** All

ACL Group Configuration

These commands allow you to compile one or more ACLs into an ACL group. Once you create an ACL group, you can assign the ACL group to one or more ports.

Table 192. ACL Group Configuration Commands

Command Syntax and Usage
`access-control group <1-256> list <1-256>` Adds the selected ACL to the ACL group. **Command mode:** Global configuration
`no access-control group <1-256> list <1-256>` Removes the selected ACL from the ACL group. **Command mode:** Global configuration
`show access-control group <1-256>` Displays the current ACL group parameters. **Command mode:** All

ACL Metering Configuration

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

Table 193. ACL Metering Configuration Commands

Command Syntax and Usage
`access-control list <1-256> meter committed-rate <64-10000000>` Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
`access-control list <1-256> meter maximum-burst-size <32-4096>` Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096 **Command mode:** Global configuration
[no] `access-control list <1-256> meter enable` Enables or disables ACL Metering. **Command mode:** Global configuration
`access-control list <1-256> meter action {drop|pass}` Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
`default access-control list <1-256> meter` Sets the ACL meter configuration to its default values. **Command mode:** Global configuration

Table 193. ACL Metering Configuration Commands

Command Syntax and Usage
`no access-control list <1-256> meter` Deletes the selected ACL meter. **Command mode:** Global configuration
`show access-control list <1-256> meter` Displays current ACL Metering parameters. **Command mode:** All

ACL Re-Mark Configuration

You can choose to re-mark IP header data for the selected ACL or ACL group. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

Table 194. ACL Re-Marking Configuration Commands

Command Syntax and Usage
`access-control list <1-256> re-mark dot1p <0-7>` Defines 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`no access-control list <1-256> re-mark dot1p` Disables use of 802.1p value for re-marked packets. **Command mode:** Global configuration
`[no] access-control list <1-256> re-mark use-tos-precedence` Enable or disable 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 <1-256> re-mark` Sets the ACL Re-mark configuration to its default values. **Command mode:** Global configuration
`show access-control list <1-256> re-mark` Displays current Re-mark parameters. **Command mode:** All

Re-Marking In-Profile Configuration

Table 195. ACL Re-Mark In-Profile Commands

Command Syntax and Usage
`access-control list <1-256> re-mark in-profile dscp <0-63>` Sets the DiffServ Code Point (DSCP) of in-profile packets to the selected value. **Command mode:** Global configuration
`no access-control list <1-256> re-mark in-profile dscp` Disables use of DSCP value for in-profile traffic. **Command mode:** Global configuration
`show access-control list <1-256> re-mark` Displays current Re-mark parameters. **Command mode:** All

Re-Marking Out-of-Profile Configuration

Table 196. ACL Re-Mark Out-of-Profile Commands

Command Syntax and Usage
`access-control list <1-256> re-mark out-profile dscp <0-63>` Sets the DiffServ Code Point (DSCP) of out-of-profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets. **Command mode:** Global configuration
`no access-control list <1-256> re-mark out-profile dscp` Disables use of DSCP value for out-of-profile traffic. **Command mode:** Global configuration
`show access-control list <1-256> re-mark` Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking Configuration

You can choose to re-mark IP header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within the ACL metering profile, or out of the ACL metering profile.

Table 197. IPv6 General Re-Mark 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] no access-control list6 <1-128> re-mark use-tos-precedence` Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`default access-control list6 <1-128> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128> re-mark` Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking In-Profile Configuration

Table 198. IPv6 Re-Mark In-Profile Options

Command Syntax and Usage
`[no] 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

Port Mirroring

Port mirroring is disabled by default. For more information about port mirroring on the CN4093, see “Appendix A: Troubleshooting” in the *IBM Networking OS 7.5 Application Guide*.

Note: Traffic on VLAN 4095 is not mirrored to the external ports.

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 199. Port Mirroring Configuration Commands

Command Syntax and Usage
`[no] port-mirroring enable` Enables or disables port mirroring. **Command mode:** Global configuration
`show port-mirroring` Displays current settings of the mirrored and monitoring ports. **Command mode:** All

Port-Mirroring Configuration

Table 200. Port-Based Port-Mirroring Configuration Commands

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

Layer 2 Configuration

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

Table 201. Layer 2 Configuration Commands

Command Syntax and Usage
`vlan` *<VLAN number>* Enter VLAN configuration mode. To view command options, see page 309. **Command mode:** Global configuration
`spanning-tree mode disable` When enabled, globally turns Spanning Tree `off` (selects Spanning-Tree mode “disable”). All ports are placed into forwarding state. Any BPDU’s received are flooded. BPDU Guard is not affected by this command. To enable Spanning-Tree, select another Spanning-Tree mode. **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**: 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 loopguard` Enables or disables Spanning Tree Loop Guard. **Command mode:** Global configuration
`show layer2` Displays current Layer 2 parameters. **Command mode:** All

802.1X Configuration

These commands allow you to configure the CN4093 as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 202. 802.1x Configuration Commands

Command Syntax and Usage
`dot1x enable` Globally enables 802.1X. **Command mode:** Global configuration
`no dot1x enable` Globally disables 802.1X. **Command mode:** Global configuration
`show dot1x` Displays current 802.1X parameters. **Command mode:** All

802.1X Global Configuration

The global 802.1X commands allow you to configure parameters that affect all ports in the CN4093.

Table 203. 802.1X Global Configuration Commands

Command Syntax and Usage
`dot1x mode [force-unauthorized|auto|force-authorized]` Sets the type of access control for all ports: – `force-unauthorized` - the port is unauthorized unconditionally. – `auto` - the port is unauthorized until it is successfully authorized by the RADIUS server. – `force-authorized` - the port is authorized unconditionally, allowing all traffic. The default value is `force-authorized`. **Command mode:** Global configuration
`dot1x quiet-time <0-65535>` Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Global configuration
`dot1x transmit-interval <1-65535>` Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds. **Command mode:** Global configuration

Table 203. 802.1X Global Configuration Commands

Command Syntax and Usage
`dot1x supplicant-timeout` <*1-65535*> Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds. **Command mode:** Global configuration
`dot1x server-timeout` <*1-65535*> Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `radius-server timeout` <*timeout-value*> (default is 3 seconds). **Command mode:** Global configuration
`dot1x max-request` <*1-10*> Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. **Command mode:** Global configuration
`dot1x re-authentication-interval` <*1-604800*> Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Global configuration
`dot1x re-authenticate` Sets the re-authentication status to `on`. The default value is `off`. **Command mode:** Global configuration
`[no] dot1x re-authenticate` Sets the re-authentication status to `off`. The default value is `off`. **Command mode:** Global configuration
`[no] dot1x vlan-assign` Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. **Command mode:** Global configuration
`default dot1x` Resets the global 802.1X parameters to their default values. **Command mode:** Global configuration
`show dot1x` Displays current global 802.1X parameters. **Command mode:** All

802.1X Guest VLAN Configuration

The 802.1X Guest VLAN commands allow you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 204. 802.1X Guest VLAN Configuration Commands

Command Syntax and Usage
[no] dot1x guest-vlan vlan <*VLAN number*> Configures the Guest VLAN number. **Command mode:** Global configuration
dot1x guest-vlan enable Enables the 802.1X Guest VLAN. **Command mode:** Global configuration
no dot1x guest-vlan enable Disables the 802.1X Guest VLAN. **Command mode:** Global configuration
show dot1x Displays current 802.1X parameters. **Command mode:** All

802.1X Port Configuration

The 802.1X port commands allows you to configure parameters that affect the selected port in the CN4093. These settings override the global 802.1X parameters.

Table 205. 802.1X Port Commands

Command Syntax and Usage
dot1x mode force-unauthorized|auto|force-authorized Sets the type of access control for the port: – force-unauthorized - the port is unauthorized unconditionally. – auto - the port is unauthorized until it is successfully authorized by the RADIUS server. – force-authorized - the port is authorized unconditionally, allowing all traffic. The default value is force-authorized. **Command mode:** Interface port
dot1x quiet-time <*0-65535*> Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds. **Command mode:** Interface port

Table 205. 802.1X Port Commands

Command Syntax and Usage
`dot1x transmit-interval` <*1-65535*> Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds. **Command mode:** Interface port
`dot1x supplicant-timeout` <*1-65535*> Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is 30 seconds. **Command mode:** Interface port
`dot1x server-timeout` <*1-65535*> Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of the `radius-server timeout` command. **Command mode:** Interface port
`dot1x max-request` <*1-10*> Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. **Command mode:** Interface port
`dot1x re-authentication-interval` <*1-604800*> Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds. **Command mode:** Interface port
`dot1x re-authenticate` Sets the re-authentication status to `on`. The default value is `off`. **Command mode:** Interface port
`[no] dot1x re-authenticate` Sets the re-authentication status `off`. The default value is `off`. **Command mode:** Interface port
`[no] dot1x vlan-assign` Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. **Command mode:** Interface port

Table 205. 802.1X Port Commands

Command Syntax and Usage
`default dot1x` Resets the 802.1X port parameters to their default values. **Command mode:** Interface port
`dot1x apply-global` Applies current global 802.1X configuration parameters to the port. **Command mode:** Interface port
`show interface port` <*port alias or number*> `dot1x` Displays current 802.1X port parameters. **Command mode:** All

RSTP/MSTP/PVRST Configuration

IBM Networking OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups, each with its own topology.

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MRST 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 206. Multiple Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree mstp 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:** Global configuration
`spanning-tree mstp version` *<0-65535>* Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within an MSTP region must have the same version number. **Command mode:** Global configuration
`spanning-tree mstp maximum-hop` *<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
`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 STP/PVRST+. When you select `spanning-tree 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
`show spanning-tree mstp mrst` Displays the current RSTP/MSTP/PVRST+ configuration. **Command mode:** All

Common Internal Spanning Tree Configuration

Table 207 describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 207. CIST Configuration Commands

Command Syntax and Usage
`default spanning-tree mstp cist` Resets all CIST parameters to their default values. **Command mode:** Global configuration
`show spanning-tree mstp cist` Displays the current CIST configuration. **Command mode:** All

CIST Bridge Configuration

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST+.

Table 208. CIST Bridge Configuration Commands

Command Syntax and Usage
`spanning-tree mstp cist-add-vlan <`*VLAN no.*`>` Add the specified VLANs to CIST. **Command mode:** Global configuration
`spanning-tree mstp cist-bridge priority <`*0-65535*`>` Configures the CIST bridge priority. 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...), and the default value is 61440. **Command mode:** Global configuration
`spanning-tree mstp cist-bridge maximum-age <`*6-40*`>` Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds. **Command mode:** Global configuration

Table 208. CIST Bridge Configuration Commands

Command Syntax and Usage
`spanning-tree mstp cist-bridge forward-delay <4-30>` Configures the CIST 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 listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. **Command mode:** Global configuration
`show spanning-tree mstp cist` Displays the current CIST bridge configuration. **Command mode:** All

CIST Port Configuration

CIST port parameters are used to modify MSTP operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+. For each port, RSTP/MSTP is turned on by default.

Table 209. CIST Port Configuration Commands

Command Syntax and Usage
`spanning-tree mstp cist interface-priority <0-240>` Configures the CIST 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 range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128. **Command mode:** Interface port
`spanning-tree mstp cist path-cost <0-200000000>` Configures the CIST 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: – 100Mbps = 200000 – 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
`spanning-tree mstp cist hello <1-10>` Configures the CIST port Hello time.The Hello time specifies how often the root 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

Table 209. CIST Port Configuration Commands (continued)

Command Syntax and Usage
`[no] spanning-tree mstp cist 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
`spanning-tree mstp cist enable` Enables MRST on the port. **Command mode:** Interface port
`no spanning-tree mstp cist enable` Disables MRST on the port. **Command mode:** Interface port
`show interface port` <*port alias or number*> `spanning-tree mstp cist` Displays the current CIST port configuration. **Command mode:** All

Spanning Tree Configuration

IBM Networking OS supports the IEEE 802.1D Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG reserved for management).

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

Table 210. Spanning Tree Configuration Commands

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

Table 210. Spanning Tree Configuration Commands

Command Syntax and Usage
`no spanning-tree stp <STG number> enable` Globally disables Spanning Tree Protocol. **Command mode:** Global configuration
`default spanning-tree <STG number>` Restores a Spanning Tree instance to its default configuration. **Command mode:** Global configuration
`[no] spanning-tree loopguard` Enables or disables spanning tree loop guard. **Command mode:** Global configuration
`show spanning-tree stp <STG number>` Displays current Spanning Tree Protocol parameters. **Command mode:** All

Bridge Spanning Tree 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 211. Bridge Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree stp <STG number> 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. The default value is 65534. **RSTP/MSTP**: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 61440. **Command mode:** Global configuration
`spanning-tree stp <STG number> bridge hello-time <1-10>` Configures the bridge Hello time.The Hello time specifies how often the root 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

Table 211. Bridge Spanning Tree Configuration Commands

Command Syntax and Usage
`spanning-tree stp <STG number> 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
`spanning-tree stp <STG number> 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 listening state to the learning state and from the learning state 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 stp <STG number> bridge` Displays the current bridge STG parameters. **Command mode:** All

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

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

Spanning Tree Port Configuration

By default for STP/PVST+, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports. By default for RSTP/MSTP, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports, with internal ports configured as Edge ports. STG port parameters include:

- Port priority
- Port path cost

For more information about port Spanning Tree commands, see "Port Spanning Tree Configuration" on page 251.

Table 212. Spanning Tree Port Commands

Command Syntax and Usage
`spanning-tree stp` *<STG number>* `priority` *<0-255>* 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...). **Command mode:** Interface port
`spanning-tree stp` *<STG number>* `path-cost` *<1-65535, 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: – 100Mbps = 19 – 1Gbps = 4 – 10Gbps = 2 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
`spanning-tree stp 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
`[no] spanning-tree edge` Enables or disables this port as an 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). **Command mode:** Interface port
`spanning-tree stp` *<STG number>* `enable` Enables STG on the port. **Command mode:** Interface port

Table 212. Spanning Tree Port Commands (continued)

Command Syntax and Usage
`no spanning-tree stp <STG number> enable` Disables STG on the port. **Command mode:** Interface port
`show interface port <port alias or number> spanning-tree stp <STG number>` Displays the current STG port parameters. **Command mode:** All

Forwarding Database Configuration

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

Table 213. FDB Configuration Commands

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
`[no] mac-address-table mac-notification` Enables or disables MAC address notification. **Command mode**: Global configuration
`show mac-address-table` Display current FDB configuration. **Command mode**: All

Static FDB Configuration

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

Table 214. FDB Configuration Commands

Command Syntax and Usage
`mac-address-table static` *<MAC address>* `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>* *<VLAN number>* Deletes a permanent FDB entry. **Command mode**: Global configuration
`no mac-address-table static all` Clears all static FDB entries. **Command mode**: Global configuration
`show mac-address-table` Display current FDB configuration. **Command mode**: All

Static Multicast MAC Configuration

The following options are available to control the forwarding of known and unknown multicast packets:

- All multicast packets are flooded to the entire VLAN. This is the default switch behavior.
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are flooded to the entire VLAN. To configure this option, define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
- Known multicast packets are forwarded only to those ports specified. Unknown multicast packets are dropped. To configure this option:
  - Define the Multicast MAC address for the VLAN and specify ports that are to receive multicast packets (`mac-address-table multicast`).
  - Enable Flood Blocking on ports that are not to receive multicast packets (`interface port` *x*) (`flood-blocking`).

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

Table 215. Static Multicast MAC Configuration Commands

Command Syntax and Usage
`mac-address-table multicast` *<MAC address> <VLAN number> <port alias or number>* Adds a static multicast entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen (-). For example: `mac-address-table multicast 01:00:00:23:3f:01 200 int1-int4` **Command mode**: Global configuration
`no mac-address-table multicast` *<MAC address> <VLAN number> <port alias or number>* Deletes a static multicast entry. **Command mode**: Global configuration
`no mac-address-table multicast {all|mac` *<MAC address>*`|vlan` *<VLAN number>*`|port` *<port alias or number>*`}` Clears static multicast entries. **Command mode**: Global configuration
`show mac-address-table multicast` Display the current static multicast entries. **Command mode**: All

Edge Control Protocol Configuration

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

Table 216. ECP Configuration Options

Command Syntax and Usage
`ecp retransmit-interval <100-9000>` Sets the retransmission interval, in milliseconds. The default value is 1000ms. **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 217. LLDP Configuration Commands

Command Syntax and Usage
`lldp refresh-interval <5-32768>` Configures the message transmission interval, in seconds. The default value is 30 seconds. **Command mode**: Global configuration
`lldp holdtime-multiplier <2-10>` Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is 4. **Command mode**: Global configuration
`lldp trap-notification-interval <1-3600>` Configures the trap notification interval, in seconds. The default value is 5. **Command mode**: Global configuration
`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

Table 217. LLDP Configuration Commands

Command Syntax and Usage
`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` Display current LLDP configuration. **Command mode**: All

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 218. LLDP Port Commands

Command Syntax and Usage
`lldp admin-status {disabled|tx_only|rx_only|tx_rx}` Configures the LLDP transmission type for the port, as follows: – Transmit only – Receive only – Transmit and receive – Disabled The default setting is `tx_rx`. **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 219. Optional TLV Commands

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
`[no] lldp tlv powermdi` Enables or disables the Power via MDI information type. **Command mode**: Interface port

Table 219. Optional TLV Commands (continued)

Command Syntax and Usage
`[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 Data Center Bridging Capability Exchange (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 CN4093 10Gb Converged Scalable Switches or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 64 trunk groups can be configured on the CN4093, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 16 ports can belong to the same trunk group.
- Configure all ports in a trunk group with the same properties (speed, duplex, flow control, STG, VLAN, and so on).
- Trunking from non-BLADE devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 220. Trunk Configuration Commands

Command Syntax and Usage
`portchannel` *<1-64>* `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` *<1-64>* `port` *<port alias or number>* Removes a physical port or ports from the current trunk group. **Command mode:** Global configuration

Table 220. Trunk Configuration Commands (continued)

Command Syntax and Usage
[no] portchannel <*1-64*> enable Enables or Disables the current trunk group. **Command mode:** Global configuration
no portchannel <*1-64*> Removes the current trunk group configuration. **Command mode:** Global configuration
show portchannel <*1-64*> Displays current trunk group parameters. **Command mode:** All

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the CN4093. Trunk hash parameters are set globally for the CN4093. 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 221 combined with the hash parameters listed in Table 222.

Table 221. Trunk Hash Settings

Command Syntax and Usage
`[no] portchannel thash ingress` Enables or disables use of the ingress port to compute the trunk hash value. The default setting is `disabled`. **Command mode:** Global configuration
`[no] portchannel thash L4port` Enables or disables use of Layer 4 service ports (TCP, UDP, etc.) to compute the hash value. The default setting is `disabled`. **Command mode:** Global configuration
`show portchannel hash` Display current trunk hash configuration. **Command mode**: All

Layer 2 Trunk Hash

Layer 2 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SMAC and DMAC

Use the following commands to configure Layer 2 trunk hash parameters for the switch.

Table 222. Layer 2 Trunk Hash Options

Command Syntax and Usage
`[no] portchannel thash l2hash l2-source-mac-address` Enables or disables Layer 2 trunk hashing on the source MAC. **Command mode:** Global configuration
`[no] portchannel thash l2hash l2-destination-mac-address` Enables or disables Layer 2 trunk hashing on the destination MAC. **Command mode:** Global configuration

Table 222. Layer 2 Trunk Hash Options (continued)

Command Syntax and Usage
`[no] portchannel thash l2hash l2-source-destination-mac` Enables or disables Layer 2 trunk hashing on both the source and destination MAC. **Command mode:** Global configuration
`show portchannel hash` Displays the current trunk hash settings. **Command mode:** All

Layer 3 Trunk Hash

Layer 3 trunk hash parameters are set globally. You can enable one or both parameters, to configure any of the following valid combinations:

- SIP (source IP only)
- DIP (destination IP only)
- SIP and DIP

Use the following commands to configure Layer 3 trunk hash parameters for the switch.

Table 223. Layer 3 Trunk Hash Options

Command Syntax and Usage
`[no] portchannel thash l3thash l3-use-l2-hash` Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared. **Command mode:** Global configuration
`[no] portchannel thash l3thash l3-source-ip-address` Enables or disables Layer 3 trunk hashing on the source IP address. **Command mode:** Global configuration
`[no] portchannel thash l3thash l3-destination-ip-address` Enables or disables Layer 3 trunk hashing on the destination IP address. **Command mode:** Global configuration
`[no] portchannel thash l3thash l3-source-destination-ip` Enables or disables Layer 3 trunk hashing on both the source and the destination IP address. **Command mode:** Global configuration
`show portchannel hash` Displays the current trunk hash settings. **Command mode:** All

Virtual Link Aggregation Group Protocol 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 224. 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. **Command mode:** Global configuration
`vlag priority <0-65535>` Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch. **Command mode:** Global configuration
`vlag startup-delay <seconds>` Sets the vLAG startup delay interval, in seconds. **Command mode:** Global configuration
`show vlag information` Displays current vLAG parameters. **Command mode:** All

vLAG Health Check Configuration

These commands allow you to configure a health check of synchronization between vLAG peers.

Table 225. vLAG Health Check Configuration Options

Command Syntax and Usage
`vlag hlthchk peer-ip <IP address>` Configures the IP address of the vLAG peer. **Command mode:** Global configuration
`[no] vlag hlthchk connect-retry-interval <1-300>` Sets in seconds the vLAG health check connect retry interval, in seconds. 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 the time between vLAG keep alive attempts, in seconds. 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 226. vLAG ISL Configuration Options

Command Syntax and Usage
`[no] vlag isl portchannel <1-64> enable` 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
`[no] vlag isl vlan <1-4094>` Enables or disables vLAG Inter-Switch Link (ISL) on the VLAN. This VLAN is used to carry VLAG protocol data. **Command mode:** Global configuration
`show vlag information` 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 CN4093.

Table 227. Link Aggregation Control Protocol Commands

Command Syntax and Usage
`lacp system-priority` <*1-65535*> Defines the priority value for the CN4093. 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:** It is recommended that you use a timeout value of `long`, to reduce LACPDU processing. If your CN4093'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 228. Link Aggregation Control Protocol Commands

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
`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
`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
`port-channel min-links <`*1-16*`>` 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
`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 Networking OS Application Guide*.

Table 229. Layer 2 Failover Configuration Commands

Command Syntax and Usage
`failover vlan` Globally turns VLAN monitor `on`. When the VLAN Monitor is `on`, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is `off`. **Command mode:** Global configuration
`no failover vlan` Globally turns VLAN monitor `off`. When the VLAN Monitor is `on`, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is `off`. **Command mode:** Global configuration
`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 230. Failover Trigger Configuration Commands

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

Auto Monitor Configuration

Table 231. Auto Monitor Configuration Commands

Command Syntax and Usage
failover trigger <*1-8*> amon portchannel <*trunk group number*> Adds a trunk group to the Auto Monitor. **Command mode:** Global configuration
no failover trigger <*1-8*> amon portchannel <*trunk group number*> Removes a trunk group from the Auto Monitor. **Command mode:** Global configuration
failover trigger <*1-8*> amon adminkey <*1-65535*> Adds a LACP *admin key* to the Auto Monitor. LACP trunks formed with this *admin key* will be included in the Auto Monitor. **Command mode:** Global configuration
no failover trigger <*1-8*> amon adminkey <*1-65535*> Removes a LACP *admin key* from the Auto Monitor. **Command mode:** Global configuration

Failover Manual Monitor Port Configuration

Use these commands to define the port link(s) to monitor. The Manual Monitor Port configuration accepts only external uplink ports.

Note: AMON and MMON configurations are mutually exclusive.

Table 232. Failover Manual Monitor Port Commands

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 to the Manual Monitor Port configuration. **Command mode:** Global configuration
`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 internal and external ports, but not management ports.

Table 233. Failover Manual Monitor Control Commands

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 to 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
`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 Networking OS 7.5 Application Guide*.

Table 234. Hot Links Configuration Commands

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 <*10-1000*> 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 235. Hot Links Trigger Configuration Commands

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 236. Hot Links Master Configuration Commands

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 237. Hot Links Backup Configuration Commands

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. Internal server ports and external uplink ports are members of VLAN 1 by default. Up to 4094 VLANs can be configured on the CN4093.

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

Table 238. VLAN Configuration Commands

Command Syntax and Usage
`vlan` *<VLAN number>* Enter VLAN configuration mode. **Command mode:** Global configuration
`protocol-vlan` *<1-8>* Configures the Protocol-based VLAN (PVLAN). **Command mode:** VLAN
`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
`stg` *<STG number>* Assigns a VLAN to a Spanning Tree Group. **Command mode:** VLAN
`[no] vmap` *<1-128>* `[extports|intports]` Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN. **Command mode:** VLAN
`member` *<port alias or number>* Adds port(s) to the VLAN membership. **Command mode:** VLAN
`no member` *<port alias or number>* Removes port(s) from this VLAN. **Command mode:** VLAN
`[no] management` Configures this VLAN as a management VLAN. You must add the management ports (for example, MGT1) to each new management VLAN. External ports cannot be added to management VLANs. **Command mode:** VLAN

Table 238. VLAN Configuration Commands (continued)

Command Syntax and Usage
`[no] flood` Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is `enabled`. **Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group. **Command mode:** VLAN
`[no] cpu` Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: – If no Mrouter is present, drop subsequent packets with same IPMC. – If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is `enabled`. **Note**: If both `flood` and `cpu` are disabled, then the switch drops all unregistered IPMC traffic. **Command mode:** VLAN
`[no] optflood` Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is `disabled`. **Command mode:** VLAN
`enable` Enables this VLAN. **Command mode:** VLAN
`no enable` Disables this VLAN without removing it from the configuration. **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`.

Protocol-Based VLAN Configuration

Use the following commands to configure Protocol-based VLAN for the selected VLAN.

Table 239. Protocol VLAN Configuration Commands

Command Syntax and Usage
`protocol-vlan <1-8> frame-type {ether2|llc|snap} <Ethernet type>` Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as `0080` (IPv4). **Command mode:** VLAN
`protocol-vlan <1-8> protocol <protocol type>` Selects a pre-defined protocol, as follows: – `decEther2`:DEC Local Area Transport – `ipv4Ether2`:Internet IP (IPv4) – `ipv6Ether2`:IPv6 – `ipx802.2`:Novell IPX 802.2 – `ipx802.3`:Novell IPX 802.3 – `ipxEther2`:Novell IPX – `ipxSnap`:Novell IPX SNAP – `netbios`:NetBIOS 802.2 – `rarpEther2`:Reverse ARP – `sna802.2`:SNA 802.2 – `snaEther2`:IBM SNA Service on Ethernet – `vinesEther2`:Banyan VINES – `xnsEther2`:XNS Compatibility **Command mode:** VLAN
`protocol-vlan <1-8> priority <0-7>` Configures the priority value for this PVLAN. **Command mode:** VLAN
`protocol-vlan <1-8> member <port alias or number>` Adds a port to the selected PVLAN. **Command mode:** VLAN
`no protocol-vlan <1-8> member <port alias or number>` Removes a port from the selected PVLAN. **Command mode:** VLAN
[no] `protocol-vlan <1-8> tag-pvlan <port alias or number>` Defines a port that will be tagged by the selected protocol on this VLAN. **Command mode:** VLAN

Table 239. Protocol VLAN Configuration Commands (continued)

Command Syntax and Usage
`protocol-vlan <1-8> enable` Enables the selected protocol on the VLAN. **Command mode:** VLAN
`no protocol-vlan <1-8> enable` Disables the selected protocol on the VLAN. **Command mode:** VLAN
`no protocol-vlan <1-8>` Deletes the selected protocol configuration from the VLAN. **Command mode:** VLAN
`show protocol-vlan <1-8>` Displays current parameters for the selected PVLAN. **Command mode:** All

Private VLAN Configuration

Use the following commands to configure Private VLAN.

Table 240. Private VLAN Configuration Commands

Command Syntax and Usage
`private-vlan type primary` Configures 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
`private-vlan type community` Configures 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
`private-vlan type isolated` Configures the VLAN type as an isolated VLAN. The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. **Command mode:** VLAN
`no private-vlan type` Clears the private-VLAN type. **Command mode:** VLAN

Table 240. Private VLAN Configuration Commands (continued)

Command Syntax and Usage
`[no] private-vlan map [<2-4094>]` Configures Private VLAN mapping between a secondary VLAN and a primary VLAN. Enter the primary VLAN ID. Secondary VLANs have the `type` defined as `isolated` or `community`. Use the `no` form to remove the mapping between the secondary VLAN and the primary VLAN. **Command mode:** VLAN
`private-vlan enable` Enables the private VLAN. **Command mode:** VLAN
`no private-vlan enable` Disables the Private VLAN. **Command mode:** VLAN
`show private-vlan [<2-4094>]` Displays current parameters for the selected Private VLAN(s). **Command mode:** VLAN

Layer 3 Configuration

The following table describes basic Layer 3 Configuration commands. The following sections provide more detailed information and commands.

Table 241. Layer 3 Configuration Commands

Command Syntax and Usage
`interface ip <interface number>` Configures the IP Interface. The CN4093 supports up to 128 IP interfaces.To view command options, see page 315. **Command mode:** Global configuration
`route-map {<1-32>}` Enter IP Route Map mode. To view command options, see page 324. **Command mode:** Global configuration
`router rip` Configures the Routing Interface Protocol. To view command options, see page 327. **Command mode:** Global configuration
`router ospf` Configures OSPF. To view command options, see page 331. **Command mode:** Global configuration
`ipv6 router ospf` Enters OSPFv3 configuration mode. To view command options, see page 384. **Command mode:** Global configuration
`router bgp` Configures Border Gateway Protocol. To view command options, see page 340. **Command mode:** Global configuration
`router vrrp` Configures Virtual Router Redundancy. To view command options, see page 367. **Command mode:** Global configuration
`ip pim component <1-2>` Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see page 379. **Command mode:** Global configuration

Table 241. Layer 3 Configuration Commands

Command Syntax and Usage
`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 CN4093 supports up to 128 IP interfaces. Each IP interface represents the CN4093 on an IP subnet on your network. The Interface option is disabled by default.

IP Interface 127 and 128 are reserved for switch management. If the IPv6 feature is enabled on the switch, IP Interface 125 and 126 are also reserved.

Note: To maintain connectivity between the management module and the CN4093, use the management module interface to change the IP address of the switch.

Table 242. IP Interface Configuration Commands

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)>* [*<IP6 prefix length (1-128)>*] [`enable`|`anycast`] 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

Table 242. IP Interface Configuration Commands (continued)

Command Syntax and Usage
`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. **Command mode:** Interface IP
[`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 243. 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 243. IPv6 Neighbor Discovery Configuration Options (continued)

Command Syntax and Usage
[no] ipv6 nd ra-intervalmin <*3-1350*> Configures the Router Advertisement minimum interval. The default value is 198 seconds. **Note**: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval. **Command mode:** Interface IP
[no] ipv6 nd 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 4 IPv4 gateways. Gateways 1–4 are reserved for default gateways. Gateway 4 is reserved for switch management.

This option is disabled by default.

Table 244. Default Gateway Configuration Commands

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

Table 244. Default Gateway Configuration Commands (continued)

Command Syntax and Usage
`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 245. IPv4 Static Route Configuration Commands

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

Table 245. IPv4 Static Route Configuration Commands (continued)

Command Syntax and Usage
`no ip route destination-address` *<IP address>* Clears all IP static routes with this destination. **Command mode:** Global configuration
`no ip route gateway` *<IP address>* Clears all IP static routes that use this gateway. **Command mode:** Global configuration
`ip route interval` *<1-60>* Configures the ping interval for ECMP health checks, in seconds. The default value is one second. **Command mode:** Global configuration
`ip route retries` *<1-60>* Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is 3. **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 and IGMP Snooping/ Relay must be enabled.

Table 246. IP Multicast Route Configuration Commands

Command Syntax and Usage
`ip mroute` *<IPMC destination> <VLAN number> <port alias or number>* {`primary`|`backup`|`host`} [*<virtual router ID>*|`none`] Adds a static multicast route. The destination address, VLAN, and member port of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router. **Command mode:** Global configuration
`no ip mroute` *<IPMC destination> <VLAN number> <port alias or number>* {`primary`|`backup`|`host`} [*<virtual router ID>*|`none`] Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified. **Command mode:** Global configuration

Table 246. IP Multicast Route Configuration Commands (continued)

Command Syntax and Usage
`ip mroute` *<IP address>* *<VLAN number>* `portchannel` *<trunk group number>* {`primary`|`backup`|`host`} [*<virtual router ID>*|`none`] Adds a static multicast route. The destination address, VLAN, and member trunk group of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router. **Command mode:** Global configuration
`no ip mroute` *<IP address>* *<VLAN number>* `portchannel` *<trunk group number>* {`primary`|`backup`|`host`} [*<virtual router ID>*|`none`] 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>* {`primary`|`backup`|`host`} [*<virtual router ID>*|`none`] Adds a static multicast route. The destination address, VLAN, and LACP *admin key* of the route must be specified. Indicate whether the route is used for a primary, backup, or host multicast router. **Command mode:** Global configuration
`no ip mroute` *<IP address>* *<VLAN number>* `adminkey` *<1-65535>*|`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
`no ip mroute all` Removes all static multicast routes. **Command mode:** Global configuration
`show ip mroute` Displays the current IP multicast routes. **Command mode:** All

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 247. ARP Configuration Commands

Command Syntax and Usage
`ip arp rearp` *<2-120>* Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache. The default value is 5 minutes. **Command mode:** Global configuration
`show ip arp` Displays the current ARP configurations. **Command mode:** All

ARP 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 248. ARP Static Configuration Commands

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 249. IP Forwarding Configuration Commands

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
ip routing Enables IP forwarding (routing) on the CN4093. Forwarding is turned on by default. **Command mode:** Global configuration
no ip routing Disables IP forwarding (routing) on the CN4093. **Command mode:** Global configuration
show ip routing Displays the current IP forwarding settings. **Command mode:** All

Network Filter Configuration

Table 250. IP Network Filter Configuration Commands

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 For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer. **Command mode:** Global configuration.
ip match-address *<1-256>* enable Enables the Network Filter configuration. **Command mode:** Global configuration

Table 250. IP Network Filter Configuration Commands

Command Syntax and Usage
`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

Routing Map Configuration

Note: The *map number* (1-32) represents the routing map you wish to configure.

Routing maps control and modify routing information.

Table 251. Routing Map Configuration Commands

Command Syntax and Usage
`route-map <1-32>` Enter route map configuration mode. **Command mode:** Route map
[no] `access-list <1-8>` Configures the Access List. For more information, see page 326. **Command mode:** Route map
[no] `as-path-list <1-8>` Configures the Autonomous System (AS) Filter. For more information, see page 327. **Command mode:** Route map
[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

Table 251. Routing Map Configuration Commands

Command Syntax and Usage
[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
[no] weight <*0-65534*> Sets the weight of the route map. **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 <*1-32*> Deletes the route map. **Command mode:** Route map
show route-map [<*1-32*>] Displays the current route configuration. **Command mode:** All

IP Access List Configuration

Note: The *route map number (*1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

Table 252. IP Access List Configuration Commands

Command Syntax and Usage
[no] access-list <*1-8*> match-address <*1-256*> Sets the network filter number. See "Network Filter Configuration" on page 323 for details. **Command mode:** Route map
[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 <*1-32*> 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 253. AS Filter Configuration Commands

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 <1-32> 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 254. Routing Information Protocol Commands

Command Syntax and Usage
`router rip` Enter Router RIP configuration mode. **Command mode:** Global configuration
`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

Table 254. Routing Information Protocol Commands (continued)

Command Syntax and Usage
`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

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 255. RIP Interface Commands

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 setting 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

Table 255. RIP Interface Commands (continued)

Command Syntax and Usage
[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
[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 Enables or disables password authentication. The default is disabled. **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 256. RIP Redistribution Commands

Command Syntax and Usage
`redistribute {fixed|static|ospf|eospf|ebgp|ibgp} <1-32>` 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 32 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} <1-32>` 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 32 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 257. OSPF Configuration Commands

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 page 334 to view command options. **Command mode:** Router OSPF
`ip ospf` *<interface number>* Configures the OSPF interface. See page 334 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 page 336 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 Router (ABR) load sharing and ABR failover possible. See page 337 to view command options. **Command mode:** Router OSPF
`lsdb-limit` *<LSDB limit (0-2048, 0 for no limit)>* Sets the link state database limit. **Command mode:** Router OSPF
`[no] default-information` *<1-16777214> <AS metric type (1|2)>* Sets one default route among multiple choices in an area. Negate the command to disable this configuration. **Command mode:** Router OSPF
`enable` Enables OSPF on the CN4093. **Command mode:** Router OSPF

Table 257. OSPF Configuration Commands (continued)

Command Syntax and Usage
`no enable` Disables OSPF on the CN4093. **Command mode:** Router OSPF
`show ip ospf` Displays the current OSPF configuration settings. **Command mode:** All

Area Index Configuration

Table 258. Area Index Configuration Commands

Command Syntax and Usage
`area <0-2> area-id <IP address>` Defines the IP address of the OSPF area number. **Command mode:** Router OSPF
`area <0-2> 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. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas. **Command mode:** Router OSPF
`area <0-2> 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

Table 258. Area Index Configuration Commands (continued)

Command Syntax and Usage
[no] area <*0-2*> 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 <*0-2*> 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 <*0-2*> enable Enables the OSPF area. **Command mode:** Router OSPF
no area <*0-2*> enable Disables the OSPF area. **Command mode:** Router OSPF
no area <*0-2*> Deletes the OSPF area. **Command mode:** Router OSPF
show ip ospf area <*0-2*> Displays the current OSPF configuration. **Command mode:** All

OSPF Summary Range Configuration

Table 259. OSPF Summary Range Configuration Commands

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 <0-2>` Displays the area index used by the CN4093. **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:** All

OSPF Interface Configuration

Table 260. OSPF Interface Configuration Commands

Command Syntax and Usage
`ip ospf area <0-2>` Configures the OSPF area index. **Command mode:** Interface IP
`ip ospf priority <0-255>` Configures the priority value for the CN4093'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

Table 260. OSPF Interface Configuration Commands (continued)

Command Syntax and Usage
`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
`[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

Table 260. OSPF Interface Configuration Commands (continued)

Command Syntax and Usage
`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

OSPF Virtual Link Configuration

Table 261. OSPF Virtual Link Configuration Commands

Command Syntax and Usage
`area-virtual-link <1-3> area <0-2>` 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 60 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

Table 261. OSPF Virtual Link Configuration Commands (continued)

Command Syntax and Usage
[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
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

OSPF Host Entry Configuration

Table 262. OSPF Host Entry Configuration Commands

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 <*0-2*> 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

Table 262. OSPF Host Entry Configuration Commands (continued)

Command Syntax and Usage
`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

OSPF Route Redistribution Configuration

Table 263. OSPF Route Redistribution Configuration Commands

Command Syntax and Usage
`redistribute {fixed|static|rip|ebgp|ibgp} <rmap ID (1-32)>` 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 (1-32)>` 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, negate the command. **Command mode:** Router OSPF
`show ip ospf redistribute` Displays the current route map settings. **Command mode:** All

OSPF MD5 Key Configuration

Table 264. OSPF MD5 Key Commands

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

Border Gateway Protocol Configuration

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current IBM Networking OS implementation, the CN4093 10Gb Converged Scalable Switch does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

Note: Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 265. Border Gateway Protocol Commands

Command Syntax and Usage
`router bgp` Enter Router BGP configuration mode. **Command mode:** Global configuration
`neighbor <1-12>` Configures each BGP *peer.* Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view command options, see page 341. **Command mode:** Router BGP
`as <0-65535>` Set Autonomous System number. **Command mode:** Router BGP
`local-preference <0-4294967294>` Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP. **Command mode:** Router BGP
`enable` Globally turns BGP on. **Command mode:** Router BGP

Table 265. Border Gateway Protocol Commands (continued)

Command Syntax and Usage
`no enable` Globally turns BGP off. **Command mode:** Router BGP
`show ip bgp` Displays the current BGP configuration. **Command mode:** All

BGP Peer Configuration

These commands are used 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 266. BGP Peer Configuration Commands

Command Syntax and Usage
`neighbor <1-12> remote-address <IP address>` Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0. **Command mode:** Router BGP
`neighbor <1-12> remote-as <1-65535>` Sets the remote autonomous system number for the specified peer. **Command mode:** Router BGP
`neighbor <1-12> update-source {<interface number>|loopback <1-5>}` Sets the source interface number for this peer. **Command mode:** Router BGP
`neighbor <1-12> timers hold-time <0, 3-65535>` Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180 seconds. **Command mode:** Router BGP
`neighbor <1-12> 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 <1-12> advertisement-interval <1-65535>` Sets time, in seconds, between advertisements. The default value is 60 seconds. **Command mode:** Router BGP

Table 266. BGP Peer Configuration Commands (continued)

Command Syntax and Usage
`neighbor <1-12> retry-interval <1-65535>` Sets connection retry interval, in seconds. The default value is 120 seconds. **Command mode:** Router BGP
`neighbor <1-12> 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 <1-12> 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
`neighbor <1-12> route-map in <1-32>` Adds route map into in-route map list. **Command mode:** Router BGP
`neighbor <1-12> route-map out <1-32>` Adds route map into out-route map list. **Command mode:** Router BGP
`no neighbor <1-12> route-map in <1-32>` Removes route map from in-route map list. **Command mode:** Router BGP
`no neighbor <1-12> route-map out <1-32>` Removes route map from out-route map list. **Command mode:** Router BGP
`no neighbor <1-12> shutdown` Enables this peer configuration. **Command mode:** Router BGP
`neighbor <1-12> shutdown` Disables this peer configuration. **Command mode:** Router BGP

Table 266. BGP Peer Configuration Commands (continued)

Command Syntax and Usage
`no neighbor <1-12>` Deletes this peer configuration. **Command mode:** Router BGP
`[no] neighbor <1-12> password <1-16 characters>` Configures the BGP peer password. **Command mode:** Router BGP
`[no] neighbor <1-12> 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 [<1-12>]` Displays the current BGP peer configuration. **Command mode:** All

BGP Redistribution Configuration

Table 267. BGP Redistribution Configuration Commands

Command Syntax and Usage
`[no] neighbor <1-12> redistribute default-metric <1-4294967294>` Sets default metric of advertised routes. **Command mode:** Router BGP
`[no] neighbor <1-12> 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 <1-12> redistribute rip` Enables or disables advertising RIP routes. **Command mode:** Router BGP

Table 267. BGP Redistribution Configuration Commands (continued)

Command Syntax and Usage
[no] neighbor <*1-12*> redistribute ospf Enables or disables advertising OSPF routes. **Command mode:** Router BGP
[no] neighbor <*1-12*> redistribute fixed Enables or disables advertising fixed routes. **Command mode:** Router BGP
[no] neighbor <*1-12*> redistribute static Enables or disables advertising static routes. **Command mode:** Router BGP
show ip bgp neighbor <*1-12*> redistribute Displays current redistribution configuration. **Command mode:** All

BGP Aggregation Configuration

These commands enable you to configure BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 268. BGP Aggregation Configuration Commands

Command Syntax and Usage
`aggregate-address` *<1-16> <IP address> <IP netmask>* Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0. **Command mode:** Router BGP
`aggregate-address` *<1-16>* `enable` Enables this BGP aggregation. **Command mode:** Router BGP
`no aggregate-address` *<1-16>* `enable` Disables this BGP aggregation. **Command mode:** Router BGP
`no aggregate-address` *<1-16>* Deletes this BGP aggregation. **Command mode:** Router BGP
`show ip bgp aggregate-address` [*<1-16>*] Displays the current BGP aggregation configuration. **Command mode:** All

MLD Global Configuration

Table 269 describes the commands used to configure global Multicast Listener Discovery (MLD) parameters.

Table 269. 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 Configuration
`enable` Globally turns MLD on. **Command mode:** MLD Configuration

Table 269. MLD Global Configuration Commands

Command Syntax and Usage
`no enable` Globally turns MLD off. **Command mode:** MLD Configuration
`exit` Exit from MLD configuration mode. **Command mode:** MLD Configuration
`show ipv6 mld` Displays the current MLD configuration parameters. **Command mode:** All

MLD Interface Configuration

Table 270 describes the commands used to configure MLD parameters for an interface.

Table 270. 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
`ipv6 mld dmrtr enable|disable` 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
`ipv6 mld llistnr <1-32>` Configures the Last Listener query interval. The default value is 1 second. **Command mode:** Interface IP
`ipv6 mld qintrval <2-65535>` Configures the interval for MLD Query Reports. The default value is 125 seconds. **Command mode:** Interface IP

Table 270. MLD Interface Configuration Commands (continued)

Command Syntax and Usage
`ipv6 mld qri <1000-65535>` Configures the interval for MLD Query Response Reports. The default value is 10,000 milliseconds. **Command mode:** Interface IP
`ipv6 mld robust <2-10>` 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
`ipv6 mld version <1-2>` Defines the MLD protocol version number. **Command mode:** Interface IP
`show ipv6 mld interface <interface number>` Displays the current MLD interface configuration. **Command mode:** All

IGMP Configuration

Table 271 describes the commands used to configure basic IGMP parameters.

Table 271. IGMP Configuration Commands

Command Syntax and Usage
`[no] ip igmp aggregate` Enables or disables IGMP Membership Report aggregation. **Command mode**: Global configuration
`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 349
- "IGMPv3 Configuration" on page 350
- "IGMP Relay Configuration" on page 351
- "IGMP Static Multicast Router Configuration" on page 352
- "IGMP Filtering Configuration" on page 353
- "IGMP Advanced Configuration" on page 355
- "IGMP Querier Configuration" on page 356

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 272 describes the commands used to configure IGMP Snooping.

Table 272. IGMP Snooping Configuration Commands

Command Syntax and Usage
`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
`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
`no ip igmp snoop vlan all` Removes all VLANs from IGMP Snooping. **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
`show ip igmp snoop` Displays the current IGMP Snooping parameters. **Command mode:** All

IGMPv3 Configuration

Table 273 describes the commands used to configure IGMP version 3.

Table 273. IGMP version 3 Configuration Commands

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

IGMP Relay Configuration

When you configure IGMP Relay, also configure the IGMP Relay multicast routers.

Table 274 describes the commands used to configure IGMP Relay.

Table 274. IGMP Relay Configuration Commands

Command Syntax and Usage
`ip igmp relay vlan <VLAN number>` Adds the VLAN to the list of IGMP Relay VLANs. **Command mode:** Global configuration
`no ip igmp relay vlan <VLAN number>` Removes the VLAN from the list of IGMP Relay VLANs. **Command mode:** Global configuration
`ip igmp relay report <0-150>` Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10. **Command mode:** Global configuration
`ip igmp relay enable` Enables IGMP Relay. **Command mode:** Global configuration
`no ip igmp relay enable` Disables IGMP Relay. **Command mode:** Global configuration
`show ip igmp relay` Displays the current IGMP Relay configuration. **Command mode:** All

IGMP Relay Multicast Router Configuration

Table 275 describes the commands used to configure multicast routers for IGMP Relay.

Table 275. IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
`ip igmp relay mrouter <1-2> address <IP address>` Configures the IP address of the IGMP multicast router used for IGMP Relay. **Command mode:** Global configuration
`ip igmp relay mrouter <1-2> interval <1-60>` Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2. **Command mode:** Global configuration

Table 275. IGMP Relay Mrouter Configuration Commands

Command Syntax and Usage
`ip igmp relay mrouter <1-2> retry <1-120>` Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4. **Command mode:** Global configuration
`ip igmp relay mrouter <1-2> attempt <1-128>` Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5. **Command mode:** Global configuration
`ip igmp relay mrouter <1-2> version <1-2>` Configures the IGMP version (1 or 2) of the multicast router. **Command mode:** Global configuration
`ip igmp relay mrouter <1-2> enable` Enables the multicast router. **Command mode:** Global configuration
`no ip igmp relay mrouter <1-2> enable` Disables the multicast router. **Command mode:** Global configuration
`no ip igmp relay mrouter <1-2>` Deletes the multicast router from IGMP Relay. **Command mode:** Global configuration

IGMP Static Multicast Router Configuration

Table 276 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 276. IGMP Static Multicast Router Configuration Commands

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 (1 or 2) 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

Table 276. IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
`no ip igmp mrouter all` Removes all static multicast routers. **Command mode:** Global configuration
`clear ip igmp mrouter` Clears the multicast router port table. **Command mode:** Global configuration
`show ip igmp mrouter` Displays the current IGMP Static Multicast Router parameters. **Command mode:** All

IGMP Filtering Configuration

Table 277 describes the commands used to configure an IGMP filter.

Table 277. IGMP Filtering Configuration Commands

Command Syntax and Usage
`ip igmp profile <1-16>` Configures the IGMP filter. To view command options, see page 354. **Command mode:** Global configuration
`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 278 describes the commands used to define an IGMP filter.

Table 278. IGMP Filter Definition Commands

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
`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 279 describes the commands used to configure a port for IGMP filtering.

Table 279. IGMP Filter Port Configuration Commands

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

Table 279. IGMP Filter Port Configuration Commands

Command Syntax and Usage
`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

IGMP Advanced Configuration

Table 280 describes the commands used to configure advanced IGMP parameters.

Table 280. IGMP Advanced Configuration Commands

Command Syntax and Usage
`ip igmp query-interval <1-600>` Sets the IGMP router query interval, in seconds. The default value is 125. **Command mode:** Global configuration
`ip igmp robust <2-10>` 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
`ip igmp timeout <1-255>` Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds. **Command mode:** Global configuration
`[no] ip igmp fastleave <VLAN number>` 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
`[no] ip igmp rtralert` Enables or disables the Router Alert option in IGMP messages. **Command mode:** Global configuration

IGMP Querier Configuration

Table 277. describes the commands used to configure IGMP Querier.

Table 281. IGMP Querier Configuration Options

Command Syntax and Usage
`ip igmp querier vlan <VLAN number> source-ip <IP address>` Configures the IGMP source IP address for the selected VLAN. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> 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
`ip igmp querier vlan <VLAN number> query-interval <1-608>` Configures the interval between IGMP Query broadcasts. The default value is 125 seconds. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> robustness <2-10>` 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
`ip igmp querier vlan <VLAN number> 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
`ip igmp querier vlan <VLAN number> startup-interval <1-608>` Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. **Command mode:** Global configuration
`ip igmp querier vlan <VLAN number> 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
`ip igmp querier vlan <VLAN number> version [v1|v2|v3]` Configures the IGMP version. The default version is `v3`. **Command mode:** Global configuration

Table 281. IGMP Querier Configuration Options (continued)

Command Syntax and Usage
`ip igmp querier enable` Enables IGMP Querier. **Command mode:** Global configuration
`no ip igmp querier enable` Disables IGMP Querier. **Command mode:** Global configuration
`show ip igmp querier vlan` *<VLAN number>* 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 282 describes the commands used to configure IKEv2.

Table 282. IKEv2 Options

Command Syntax and Usage
`ikev2 retransmit-interval` *<1-20>* Sets the timeout value, in seconds, 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 283 describes the commands used to configure an IKEv2 proposal.

Table 283. IKEv2 Proposal Options

Command Syntax and Usage
`ikev2 proposal` Enter IKEv2 proposal mode. **Command mode:** Global configuration
`encryption {3des|aes-cbc|des}` Configures IKEv2 encryption mode. The default value is `3des`. **Command mode:** IKEv2 proposal
`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 284 describes the commands used to configure IKEv2 preshare keys.

Table 284. 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 285 describes the commands used to configure IKEv2 identification.

Table 285. IKEv2 Identification Options

Command Syntax and Usage
`ikev2 identity local address` Configures the switch to use the supplied IPv6 address as identification. **Command mode:** Global configuration
`ikev2 identity local fqdn <1-32 characters>` Configures the switch to use the fully-qualified domain name (such as “example.com”) as identification. **Command mode:** Global configuration
`ikev2 identity local email <1-32 characters>` Configures the switch to use the supplied email address (such as “xyz@example.com”) as identification. **Command mode:** Global configuration
`show ikev2 identity` Displays the current IKEv2 identification settings. **Command mode:** All

IPsec Configuration

Table 286 describes the commands used to configure IPsec.

Table 286. 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 287 describes the commands used to configure IPsec transforms.

Table 287. 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 288 describes the commands used to configure an IPsec traffic selector.

Table 288. 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
`prefix <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 289 describes the commands used to configure an IPsec dynamic policy.

Table 289. 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

Table 289. IPsec Dynamic Policy Options (continued)

Command Syntax and Usage
`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 290 describes the commands used to configure an IPsec manual policy.

Table 290. 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. **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). **Command mode:** IPsec manual policy

Table 290. IPsec Manual Policy Options (continued)

Command Syntax and Usage
`in-esp cipher-key` *<key code (hexadecimal)>* Sets the inbound Encapsulating Security Payload (ESP) cipher key. **Command mode:** IPsec manual policy
`in-esp auth-key` *<key code (hexadecimal)>* Sets the inbound Encapsulating Security Payload (ESP) authenticator key. **Command mode:** IPsec manual policy
`in-esp auth-key spi` *<256-4294967295>* Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **Command mode:** IPsec manual policy
`out-ah auth-key` *<key code (hexadecimal)>* Sets the outbound Authentication Header (AH) authenticator key. **Command mode:** IPsec manual policy
`out-ah spi` *<256-4294967295>* Sets the outbound Authentication Header (AH) Security Parameter Index (SPI). **Command mode:** IPsec manual policy
`out-esp auth-key` *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) authenticator key. **Command mode:** IPsec manual policy
`out-esp cipher-key` *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) cipher key. **Command mode:** IPsec manual policy
`out-esp auth-key spi` *<256-4294967295>* Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **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 291. Domain Name Service Commands

Command Syntax and Usage
[no] `ip dns primary-server` <*IP address*> 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*> 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*> 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*> 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

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 two DHCP/BOOTP servers with IP addresses that have been configured on the CN4093.

BOOTP relay is turned off by default.

Table 292. Global BOOTP Relay Configuration Options

Command Syntax and Usage
[no] ip bootp-relay server <*1-4*> 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 293. 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 <*1-4*> 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

Table 293. BOOTP Relay Broadcast Domain Configuration Options

Command Syntax and Usage
`no ip bootp-relay bcast-domain <1-10>` Deletes the selected broadcast domain configuration. **Command mode:** Global configuration
`show ip bootp-relay` Displays the current parameters for the BOOTP Relay broadcast domain. **Command mode:** All

VRRP Configuration

Virtual Router Redundancy Protocol (VRRP) support on the CN4093 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 Networking 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 Networking OS 7.5 Application Guide.*

Table 294. Virtual Router Redundancy Protocol Commands

Command Syntax and Usage
`router vrrp` Enter Router VRRP configuration mode. **Command mode:** Global configuration
`[no] hot-standby` Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled. **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 295. VRRP Virtual Router Configuration Commands

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 255. 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 VRID (above) 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 `addr` option above, 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 295. VRRP Virtual Router Configuration Commands (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
[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
`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

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 296. VRRP Priority Tracking Configuration Commands

Command Syntax and Usage
[no] virtual-router <*1-128*> track virtual-routers When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default. **Command mode:** Router VRRP
[no] virtual-router <*1-128*> track interfaces When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default. **Command mode:** Router VRRP
[no] virtual-router <*1-128*> track 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 <*1-128*> track Displays the current configuration for priority tracking for this virtual router. **Command mode:** All

Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the CN4093 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 CN4093s in a hot-standby failover configuration, where only one switch is active at any time.

Table 297. VRRP Virtual Router Group Configuration Commands

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` below) 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. Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority. The *owner* parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254. **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 297. VRRP Virtual Router Group Configuration Commands (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
`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

Virtual Router Group Priority Tracking Configuration

Note: If *Virtual Router Group Tracking* is enabled, the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 298. Virtual Router Group Priority Tracking Configuration Commands

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

Table 298. Virtual Router Group Priority Tracking Configuration Commands

Command Syntax and Usage
[no] group track ports When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default. **Command mode:** Router VRRP
show ip vrrp group track Displays the current configuration for priority tracking for this virtual router. **Command mode:** All

VRRP Interface Configuration

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 299. VRRP Interface Commands

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

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

Table 300. VRRP Tracking Configuration Commands

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

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 369) are enabled.

Protocol Independent Multicast Configuration

Table 301. PIM Configuration Options

Command Syntax and Usage
`ip pim component <1-2>` Enter PIM component mode. See page 375 to view options. **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

Table 302. 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 303. 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 304. 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> <IP address>* Removes the specified static RP. **Command mode**: PIM Component

PIM Interface Configuration

Table 305. 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

Table 305. PIM Interface Configuration Options (continued)

Command Syntax and Usage
`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
`[no] 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 for which a neighbor is to consider this switch to be operative (up). The default value is 105. **Command mode**: Interface IP
`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

Table 305. PIM Interface Configuration Options (continued)

Command Syntax and Usage
`[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
`show ip pim neighbor-filters` Displays the configured PIM neighbor filters. **Command mode**: All
`show ip pim interface [`<*interface number*>`|detail]` Displays the current PIM interface parameters. **Command mode**: All

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 1 is used for data traffic.
- Gateways 3 and 4 are reserved for management.

Table 306 describes the IPv6 Default Gateway Configuration commands.

Table 306. IPv6 Default Gateway Configuration Commands

Command Syntax and Usage
`ip gateway6 {<gateway number>} 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 {<gateway number>} enable` Enables or disables the default gateway. **Command mode**: Global configuration
`no ip gateway6 {<gateway number>}` Deletes the default gateway. **Command mode**: Global configuration
`show ipv6 gateway6 {<gateway number>}` Displays the current IPv6 default gateway configuration. **Command mode**: All

IPv6 Static Route Configuration

Table 307 describes the IPv6 static route configuration commands.

Table 307. IPv6 Static Route Configuration Commands

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

Table 307. IPv6 Static Route Configuration Commands (continued)

Command Syntax and Usage

`no ip route6 [destination-address` *<IPv6 address>*`|`
`gateway` *<default gateway address>*`|interface` *<1-128>*`|all]`
Clears IPv6 static routes. You are prompted to select the routes to clear, based on the following criteria:
– **`dest`**: Destination IPv6 address of the route
– **`gw`**: Default gateway address used by the route
– **`if`**: Interface used by the route
– **`all`**: All 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 308 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 308. IPv6 Neighbor Discovery Cache Configuration Commands

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` *<1-128>*`|all interface`
`port` *<port number>*`|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 309. IPv6 Path MTU Commands

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 310. IPv6 Neighbor Discovery Prefix Commands

Command Syntax and Usage
`interface ip <1-127>` 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 the selected Neighbor Discovery prefix(es). If you specify an interface number, all prefixes for the interface are removed. **Command mode**: Interface IP

Table 310. IPv6 Neighbor Discovery Prefix Commands (continued)

Command Syntax and Usage

`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 [no-autoconfig]` Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix. The default setting is `enabled`. To clear the off-link flag, omit the off-link parameter when you issue this command. **Command mode**: Interface IP
`ipv6 nd prefix {<IPv6 prefix> <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 311. 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

Open Shortest Path First Version 3 Configuration

Table 312. OSPFv3 Configuration Commands

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
`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

Table 312. OSPFv3 Configuration Commands (continued)

Command Syntax and Usage
`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 313. 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

Table 313. OSPFv3 Area Index Configuration Options (continued)

Command Syntax and Usage
`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
`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 314. 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 315. 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 316. 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 dead-interval` *<1-65535>* Configures the health parameters of a `hello` packet, in seconds, before declaring a silent router to be 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

Table 316. OSPFv3 Interface Configuration Options (continued)

Command Syntax and Usage
`[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
`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 317. 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 317. 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 318. 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

Table 318. OSPFv3 Virtual Link Configuration Options (continued)

Command Syntax and Usage
`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 Host Entry Configuration

Table 319. 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
`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 Redist Entry Configuration

Table 320. 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

Table 320. OSPFv3 Redist Entry Configuration Options

Command Syntax and Usage
`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
`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 321. 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

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 322. IP Loopback Interface Commands

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

Table 322. IP Loopback Interface Commands (continued)

Command Syntax and Usage
`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

Converged Enhanced Ethernet Configuration

Table 323 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 323. CEE Commands

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
`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. When ETS is enabled, you cannot configure the 802.1p menu options.

ETS Global Priority Group Configuration

Table 324 describes the global ETS Priority Group configuration options.

Table 324. Global ETS Priority Group Commands

Command Syntax and Usage
`[no] cee global ets priority-group pgid` *<0-7, 15>* `bandwidth` *<bandwidth percentage (0, 10-100)>* `priority` *<802.1p priority (0-7)>* 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. **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 Priority Group parameters. **Command mode**: All

Priority Flow Control Configuration

Priority-based Flow Control (PFC) enhances flow control by allowing the switch to pause traffic based on its 802.1p priority value, while allowing traffic at other priority levels to continue.

Port-level 802.1p PFC Configuration

Table 325 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 325. Port 802.1p PFC Options

Command Syntax and Usage
`cee port` *<port alias or number>* `pfc enable` Enables Priority Flow Control on the selected port. **Command mode**: Global configuration
`no cee port` *<port alias or number>* `pfc enable` Disables Priority Flow Control on the selected port. **Command mode**: Global configuration
`cee port` *<port alias or number>* `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 or number>* `pfc priority` *<0-7>* `enable` Disables Priority Flow Control on the selected 802.1p priority. **Command mode**: Global configuration
`[no] cee port` *<port alias or number>* `pfc priority` *<0-7>* `description` *<1-31 characters>* Enter text to describe the priority value. **Command mode**: Global configuration
`show cee port` *<port alias or number>* `pfc priority` *<0-7>* Displays the current 802.1p PFC parameters for the selected port. **Command mode**: All
`show cee port` *<port alias or number>* `pfc` Displays the current PFC parameters for the selected port. **Command mode**: All

DCBX Port Configuration

Table 326 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 326. Port DCBX Commands

Command Syntax and Usage
`cee port <port alias or number> dcbx app_proto advertise` Enables or disables DCBX Application Protocol advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
`cee port <port alias or number> dcbx app_proto willing` Enables or disables Application Protocol willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
`cee port <port alias or number> dcbx ets advertise` Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
`cee port <port alias or number> dcbx ets willing` Enables or disables ETS willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
`cee port <port alias or number> dcbx pfc advertise` Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device). **Command mode**: Global configuration
`cee port <port alias or number> dcbx pfc willing` Enables or disables PFC willingness to accept configuration data from the peer device. When enabled, the Willing flag is set to 1 (willing to accept data). **Command mode**: Global configuration
`no cee port <port alias or number> dcbx enable` Disables DCBX on the port. **Command mode**: Global configuration
`cee port <port alias or number> dcbx enable` Enables DCBX on the port. **Command mode**: Global configuration
`show cee port <port alias or number> dcbx` Displays the current port DCBX parameters. **Command mode**: All

Fibre Channel Configuration

As a converged switch, the CN4093 provides combined support for Ethernet and Fibre Channel (FC) networks. Ports EXT11-EXT16 are hybrid, allowing them to operate in either Ethernet mode (the default), or in Fibre Channel mode for direct connection to Fibre Channel devices.

The CN4093 can be used in the following Fibre Channel applications:

- As an FCoE gateway for bridging FCoE and Fibre Channel networks
- As a Node Port Virtualized (NPV) Gateway for uplinking multiple Fibre Channel nodes to a full fabric switch
- As a Full-Fabric Switch — a central element of a Fibre Channel network

Table 332 describes generic Fibre Channel configuration options.

Table 327. Fibre Channel Configuration Commands

Command Syntax and Usage
`[no] system port` *<low port>*`-`*<high port>* `type fc` Enables or disables Fibre Channel mode on the specified port range. Fibre Channel can be enabled only for port pairs, specifically for: EXT11-EXT12, EXT13-EXT14 and EXT15-EXT16. Default setting is disabled (ports are in Ethernet mode). **Note:** VLAN tagging is automatically enabled on any ports placed in Fibre Channel mode. **Command mode**: Global configuration
`[no] fcalias` *<1-64 characters>* `wwn` *<port World Wide Name>* Configures or removes an FC alias name for the specified port World Wide Name. **Command mode:** Global configuration
`fcdomain domain` *<0-239>* `{preferred|static}` Configures the domain type for the specified FC domain ID: – `preferred` allows the domain ID to be re-assigned. If the switch does not get its requested domain ID, it accepts any assigned domain ID. – `static` does not allow the domain ID to be re-assigned. If the switch does not get that domain ID, it does not join the fabric. Default setting is `preferred`. **Command mode:** Global configuration
`clear zone database` Erases all FC zones and zonesets. **Command mode:** Global configuration

FC Port Configuration

Use the following commands to configure Fibre Channel ports.

Table 328. Fibre Channel Port Configuration Commands

Command Syntax and Usage
`interface fc` <*FC port alias or number*> Enter Fibre Channel port configuration mode. **Command mode:** Global configuration
`[no] shutdown` Disables or enables the FC port. Default setting is enabled (`no shutdown`) **Command mode:** FC Port configuration
`fc-speed {2|4|8|auto}` Configures the Fibre Channel port speed in Gbps or allows the port to negotiate its speed automatically. Default setting is `auto`. **Command mode:** FC Port configuration

FC VLAN Configuration

Use the following commands to configure the Fibre Channel Forwarding VLAN.

Table 329. FCF VLAN Configuration Commands

Command Syntax and Usage
`vlan` <*VLAN number*> Enter VLAN configuration mode. **Command mode:** Global configuration
`[no] fcf enable` Enables or disables the VLAN as Fibre Channel Forwarding VLAN. Default setting is disabled. **Command mode:** VLAN configuration
`[no] npv enable` Enables or disables NPV gateway functionality for the VLAN. Default setting is disabled. **Command mode:** VLAN configuration
`[no] npv traffic-map external-interface` <*port no.*> Enables or disables the selected ports as NP (external uplink) ports. **Command mode:** VLAN configuration
`fcoe fcmap` <*fabric map ID*> Configures the global FC-map that identifies the FC fabric used by the switch. The switch will discard MAC addresses that are not part of the current fabric, which avoids cross-fabric talk. The FC-map is a 24-bit hexadecimal value. The default value is 0x0efc00. **Command mode:** VLAN configuration

Table 329. FCF VLAN Configuration Commands

Command Syntax and Usage
`no fcoe fcmap` Resets the FC-map to the default 0x0efc00 value. **Command mode:** VLAN configuration
`fcoe fcf-priority <0-255>` Configures the FCF priority. When an FC initiator sends login requests to multiple FCFs, it selects the one with the highest priority value. The default value is 128. **Command mode:** VLAN configuration
`no fcoe fcf-priority` Resets the FCF priority to the default 128 value. **Command mode:** VLAN configuration
`fcoe fka-adv-period <8-90>` Configures the FIP Keep Alive advertising period, in seconds. **Command mode:** VLAN configuration

FC Zone Configuration

Use the following commands to configure Fibre Channel zones.

Table 330. Fibre Channel Zone Configuration Commands

Command Syntax and Usage
`[no] zone name <1-64 characters>` Enter FC Zone configuration mode for the specified zone. If the zone doesn't exist, it is created. The `no` form of the command erases the zone. **Command mode:** Global configuration
`zone clone <selected_zone_name> <new_zone_name>` Creates a new zone with the attributes of the selected zone. **Command mode:** Global configuration
`zone rename <current_name> <new_name>` Renames the FC zone. **Command mode:** Global configuration

Table 330. Fibre Channel Zone Configuration Commands

Command Syntax and Usage
`[no] zone default-zone permit` Permits or denies traffic flow to default zone members. **Command mode:** Global configuration
`[no] member {pwwn <pwwn>|fcid <ID number>|fcalias <alias ID>}` Adds or removes zone members based on: – `pwwn`: Port World Wide Number – `fcid`: FC ID of the port, in hex format (for example, 0xce00d1). – `fcalias`: Alias name of the FC device. **Command mode:** FC Zone configuration

FC Zoneset Configuration

Use the following commands to configure Fibre Channel zonesets.

Table 331. Fibre Channel Zoneset Configuration Commands

Command Syntax and Usage
`[no] zoneset name <1-64 characters>` Enter FC Zoneset configuration mode for the specified zone. If the zoneset doesn't exist, it is created. The `no` form of the command erases the zoneset. **Command mode:** Global configuration
`[no] zoneset activate name <1-64 characters>` Activates or deactivates the zoneset. Only one zoneset can be active at any point in time. Activating a zoneset automatically deactivates any other zoneset currently active. **Command mode:** Global configuration
`zoneset clone <selected_zoneset_name> <new_zoneset_name>` Creates a new zoneset with the attributes of the selected zoneset. **Command mode:** Global configuration
`zone copy active-zoneset running-config` Copies the active zoneset database to the running configuration. **Command mode:** Global configuration
`zoneset rename <current_name> <new_name>` Renames the FC zoneset. **Command mode:** Global configuration
`[no] member <1-64 characters>` Adds or removes a zone from the zoneset. **Command mode:** FC Zoneset configuration

Fibre Channel over Ethernet 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 332 describes the FCoE configuration options.

Table 332. FCoE Configuration Commands

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
`fcoe fips timeout-acl` Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system. **Command mode**: Global configuration
`show fcoe` 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 333 describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 333. Port FIP Snooping Commands

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). – `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`. **Note**: If IPv6 ACLs are assigned to the port, you cannot enable FCoE. **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" on page 407
- "RMON Event Configuration" on page 408
- "RMON Alarm Configuration" on page 408

RMON History Configuration

Table 334 describes the RMON History commands.

Table 334. RMON History Commands

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 335 describes the RMON Event commands.

Table 335. RMON Event Commands

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 336 describes the RMON Alarm commands.

Table 336. RMON Alarm Commands

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

Table 336. RMON Alarm Commands (continued)

Command Syntax and Usage
`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
`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 337 describes the virtualization configuration options.

Table 337. Virtualization Configurations Options

Command Syntax and Usage
`virt enable` Enables VMready. The default setting is `disabled`. **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 338 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 338. VM Bandwidth Management Options

Command Syntax and Usage
`virt vmpolicy vmbwidth` [*<MAC address>*|*<UUID>*|*<name>*|*<IP address>*|*<index number>*] `txrate` *<64-10000000> <max. burst> <ACL number>* The first `txrate` value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64. The second `txrate` value configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096. The third `txrate` value represents the ACL assigned to the transmission rate. The ACL is 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
`virt vmpolicy vmbwidth` [*<MAC address>*|*<UUID>*|*<name>*|*<IP address>*|*<index number>*] `rxrate` *<64-10000000> <max. burst>* The first `rxrate` value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64. The second `rxrate` value configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode**: Global configuration

Table 338. VM Bandwidth Management Options (continued)

Command Syntax and Usage
`[no] virt vmpolicy vmbwidth [`*<MAC address>*`|`*<UUID>*`|`*<name>*`|`*<IP address>*`|`*<index number>*`] bwctrl` Enables or disables bandwidth control on the VM policy. **Command mode**: Global configuration
`[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 339 describes the Virtual NIC (vNIC) configuration options.

Table 339. 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**: All

vNIC Port Configuration

Table 340 describes the Virtual NIC (vNIC) port configuration options.

Table 340. vNIC Port Commands

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 341 describes the Virtual NIC (vNIC) Group configuration options.

Table 341. vNIC Group Commands

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 341. vNIC Group Commands (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: `intA1.1` **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
`enable` Enables the vNIC Group. **Command mode:** vNIC Group configuration
`no enable` Disables the vNIC Group. **Command mode:** vNIC Group configuration
`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 342 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 342. VM Group Commands

Command Syntax and Usage
`virt vmgroup <1-1024> cpu` Enables or disables sending unregistered IPMC to CPU. **Command mode:** Global configuration
`virt vmgroup <1-1024> flood` Enables or disables flooding unregistered IPMC. **Command mode:** Global configuration
`virt vmgroup <1-1024> optflood` Enables or disables optimized flooding. **Command mode:** Global configuration
`virt vmgroup <1-1024> 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 an 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 <1-1024> vmap <VMAP number> intports|extports` Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external 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 269. **Command mode:** Global configuration
`[no] virt vmgroup <1-1024> tag` Enables or disables VLAN tagging on ports in this VM group. **Command mode:** Global configuration
`virt vmgroup <1-1024> 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

Table 342. VM Group Commands (continued)

Command Syntax and Usage
`no virt vmgroup` *<1-1024>* `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
`virt vmgroup` *<1-1024>* `profile` *<profile name (1-39 characters)>* Adds the selected VM profile to the VM group. **Command mode:** Global configuration
`no virt vmgroup` *<1-1024>* `profile` Removes the VM profile assigned to the VM group. **Command mode:** Global configuration
`virt vmgroup` *<1-1024>* `port` *<port number or alias>* 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` *<1-1024>* `port` *<port number or alias>* Removes the selected port from the VM group. **Command mode:** Global configuration
`virt vmgroup` *<1-1024>* `portchannel` *<trunk number>* Adds the selected trunk group to the VM group. **Command mode:** Global configuration
`no virt vmgroup` *<1-1024>* `portchannel` *<trunk number>* Removes the selected trunk group from the VM group. **Command mode:** Global configuration
`virt vmgroup` *<1-1024>* `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` *<1-1024>* `key` *<1-65535>* Removes an LACP *admin key* from the VM group. **Command mode:** Global configuration

Table 342. VM Group Commands (continued)

Command Syntax and Usage
`virt vmgroup <1-1024> stg <STG number>` Assigns the VM group VLAN to a Spanning Tree Group (STG). **Command mode:** Global configuration
`virt vmgroup <1-1024> 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 <1-1024> validate` Disables MAC address spoof prevention for the specified VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024>` Deletes the VM group. **Command mode:** Global configuration
`show virt vmgroup <1-1024>` Displays the current VM group parameters. **Command mode:** All

VM Check Configuration

Table 343 describes the VM Check validation options used for MAC address spoof prevention.

Table 343. VM Check Configuration Options

Command Syntax and Usage
`virt vmcheck acls max` <*1-256*> Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. 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
`show virt vmcheck` Displays the current VM Check settings. See page 104 for sample output. **Command mode:** Global configuration

VM Profile Configuration

Table 344 describes the VM Profiles configuration options.

Table 344. VM Profiles Commands

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 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 345 describes the VMware configuration options.When the user configures 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 345. VM Ware Commands

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 (Ciscoz 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
`show virt vmware` Displays the current VMware parameters. **Command mode:** All

Edge Virtual Bridge VSI Type Database Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). Table 345 describes the EVB VSI Type Database configuration options.

Note: EVB is supported in stacked mode starting with release 2.5.

Table 346. Edge Virtual Bridge Configuration Options

Command Syntax and Usage
`virt evb vsidb` *<VSIDB_number>* Enter Virtual Station Interface Database configuration mode. **Command mode:** Global configuration
`virt evb update vsidb` *<VSIDB_number>* Update VSI types from the VSI database. **Command mode**: All
`clear virt evb vsidb` *<VSIDB_number>* Clears local VSI types cache. **Command mode**: Privileged EXEC
`clear virt evb vsi` Clears VSI database associations. **Command mode**: Privileged EXEC
`host` *<IP address>* Sets the Virtual Station Interface Type database manager IP address. **Command mode:** VSI Database
`port` *<1-65534>* Sets the Virtual Station Interface Type database manager port. **Command mode:** VSI Database
`filename` *<URI path>* Sets the Virtual Station Interface Type database document name. **Command mode:** VSI Database
`filepath` *<URI path>* Sets the Virtual Station Interface Type database document path. **Command mode:** VSI Database
`update-interval` *<5-300>* Sets the Virtual Station Interface Type database update interval in seconds. A value of “0” disables periodic updates. **Command mode:** VSI Database
`show virt evb vsitypes [mgrid` *<0-255>* `| typeid` *<1-16777215>* `| version` *<0-255>* Displays the current Virtual Station Interface Type database parameters. **Command mode:** All

Table 346. Edge Virtual Bridge Configuration Options (continued)

Command Syntax and Usage
`show virt evb vsidb <VSIDB_number>` Displays the current Virtual Station Interface database information. **Command mode:** All
`no virt evb vsidb <VSIDB_number>` Resets the Virtual Station Interface Type database information to the default values. **Command mode:** Global configuration

Edge Virtual Bridge VSI Type Profile Configuration

Table 347 describes the Virtual Station Interface Type profile configuration options.

Table 347. Edge Virtual Bridge VSI Type Profile Configuration Options

Command Syntax and Usage
`virt evb profile <profile_number>` Enter Virtual Station Interface type profile configuration mode. **Command mode:** Global configuration
`[no] reflective-relay` Enables or disables VEPA mode (Reflective Relay capability). **Command mode:** EVB Profile
`[no] vsi-discovery` Enables or disables VSI Discovery (ECP and VDP). **Command mode:** EVB Profile
`no virt evb profile <profile_number>` Deletes the specified EVB profile. **Command mode:** Global configuration
`show virt evb profile [<1-16>]` Displays the current EVB profile parameters. **Command mode:** All
`evb profile <1-16>` Applies the specified EVB profile for the port. Automatically enables LLDP, EVB, and TLV on the corresponding port. **Command mode:** Interface port
`no evb profile` Resets EVB profile for the port. Automatically disables LLDP, EVB, and TLV on the corresponding port. **Command mode:** Interface port

Service Location Protocol Configuration

Service Location Protocol (SLP) enables networked devices to request/announce services over a local area network without prior configuration. In an SLP environment, devices may have the following roles:

- User Agents (UA) are devices requesting services.
- Service Agents (SA) are devices providing services.
- Directory Agents (DA) are devices caching services provided by SAs. When present in an SLA setup, DAs mediate all communication between UAs and SAs.

When SLP is enabled, the CN4093 10Gb Converged Scalable Switch behaves as a Service Agent providing systems management services.

Table 348. Service Location Protocol

Command Syntax and Usage
`[no] ip slp enable` Enables or disables SLP. Default value is disabled. **Command mode**: Global configuration
`[no] ip slp active-da-discovery enable` Enables or disables active directory agent discovery. Default value is disabled. **Command mode**: Global configuration
`ip slp active-da-discovery-start-wait-time` *<1-10>* Number of seconds to wait after enabling SLP before attempting active DA discovery, if active DA discovery is enabled. Default value is 3. **Command mode**: Global configuration
`clear ip slp directory-agents` Clears directory agents discovered. **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:

```
Router(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 FTP/TFTP/SFTP, as described on page 423.

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 [data-port|extm-port|mgt-port]
    or
Router(config)# copy running-config tftp [data-port|extm-port|mgt-port]
    or
Router(config)# copy running-config sftp [data-port|extm-port|mgt-port]
```

Select a port, or press **Enter** to use the default (management port). The switch prompts you for the server address and filename.

Notes:

- 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).
- If the FTP/TFTP 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 [extm-port|mgt-port|data-port]
    or
Router(config)# copy tftp running-config [extm-port|mgt-port|data-port]
    or
Router(config)# copy sftp running-config [extm-port|mgt-port|data-port]
```

Select a port, or press **Enter** to use the default (management port). 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 349. 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
`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 350. Port Operations Commands

Command Syntax and Usage
`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
`show interface port` *<port number or alias>* `operation` Displays the port interface operational state. **Command Mode**: Privileged EXEC

Operations-Level Port 802.1X Commands

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

Table 351. 802.1X Operations Commands

Command Syntax and Usage
`interface port` <*port number or alias*> `dot1x init` Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration: – `force unauth`: the port is placed in unauthorized state, and traffic is blocked. – `auto`: the port is placed in unauthorized state, then authentication is initiated. – `force auth`: the port is placed in authorized state, and authentication is not required. **Command Mode**: Privileged EXEC
`interface port` <*port number or alias*> `dot1x re-authenticate` Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as `auto`. **Command Mode**: Privileged EXEC

Operations-Level FCoE Commands

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

Table 352. FCoE Operations Commands

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

Operations-Level VRRP Commands

Table 353. Virtual Router Redundancy Operations Commands

Command Syntax and Usage
`router vrrp backup` <*virtual router number (1-255)*> 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 354. IP BGP Operations Commands

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

Protected Mode Options

Protected Mode is used to secure certain switch management options, so they cannot be changed by the management module.

Table 355. Protected Mode Options

Command Syntax and Usage
`[no] protected-mode external-management` Enables exclusive local control of switch management. When Protected Mode is set to `on`, the management module cannot be used to disable external management on the switch. The default value is `enabled`. **Note**: Due to current management module implementation, this setting cannot be disabled. **Command Mode**: Global Configuration
`[no] protected-mode external-ports` Enables exclusive local control of external ports. When Protected Mode is set to `on`, the management module cannot be used to disable external ports on the switch. The default value is `enabled`. **Note**: Due to current management module implementation, this setting cannot be disabled. **Command Mode**: Global Configuration
`[no] protected-mode factory-default` Enables exclusive local control of factory default resets. When Protected Mode is set to `on`, the management module cannot be used to reset the switch software to factory default values. The default value is `enabled`. **Note**: Due to current management module implementation, this setting cannot be disabled. **Command Mode**: Global Configuration

Table 355. Protected Mode Options (continued)

Command Syntax and Usage
`[no] protected-mode management-vlan-interface` Enables exclusive local control of the management interface. When Protected Mode is set to `on`, the management module cannot be used to configure parameters for the management interface. The default value is `enabled`. **Note**: Due to current management module implementation, this setting cannot be disabled. **Command Mode**: Global Configuration
`protected-mode enable` Turns Protected Mode `on`. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options. **Command Mode**: Global Configuration
`no protected-mode enable` Turns Protected Mode `off`. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options. **Command Mode**: Global Configuration
`show protected-mode` Displays the current Protected Mode configuration. **Command Mode**: Global Configuration

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 356. VMware Operations Commands

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**: Privileged EXEC

Table 356. VMware Operations Commands

Command Syntax and Usage
`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**: Privileged EXEC
`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**: Privileged EXEC
`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**: Privileged EXEC
`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**: Privileged EXEC
`virt vmware scan` Performs a scan of the VM Agent, and updates VM information. **Command Mode**: Privileged EXEC
`virt vmware vmacpg` *<MAC address> <Port Group name>* Changes a VM NIC's configured Port Group. **Command Mode**: Privileged EXEC

Table 356. VMware Operations Commands

Command Syntax and Usage
`virt vmware updpg` *<Port Group name> <host ID> <VLAN number> [<shaping enabled> <average Kbps> <burst KB> <peak Kbps>]* Updates a VMware host's Port Group parameters. **Command Mode**: Privileged EXEC

Distributed vSwitch Operations

Table 357 describes distributed vSwitch operations.

Table 357. Distributed vSwitch Options

Command Syntax and Usage
`virt vmware dvswitch add` *<datacenter name> <dvSwitch name> <vSwitch version>* Adds a distributed vSwitch to a datacenter. **Command Mode**: Privileged EXEC
`virt vmware dvswitch del` *<datacenter name> <dvSwitch name>* Deletes a distributed vSwitch from a datacenter. **Command Mode**: Privileged EXEC
`virt vmware dvswitch addhost` *<dvSwitch name> <host UUID, IP address, or name>* Adds a host to a distributed vSwitch. **Command Mode**: Privileged EXEC
`virt vmware dvswitch remhost` *<dvSwitch name> <host UUID, IP address, or name>* Removes a host from a distributed vSwitch. **Command Mode**: Privileged EXEC
`virt vmware dvswitch adduplnk` *<dvSwitch name> <host UUID, IP address, or name> <uplink name>* Adds a NIC to the distributed vSwitch, to use as an uplink. **Command Mode**: Privileged EXEC
`virt vmware dvswitch remuplnk` *<dvSwitch name> <host UUID, IP address, or name> <uplink name>* Removes an uplink NIC from the distributed vSwitch. **Command Mode**: Privileged EXEC

Distributed Port Group Operations

Table 358 describes distributed port group operations.

Table 358. Distributed Port Group Options

Command Syntax and Usage

`virt vmware dpg add` *<port group name> <dvSwitch name> <VLAN number>*
`[ishaping|eshaping` *<average Kbps> <burst KB> <peak Kbps>*`]`
`[ishaping|eshaping` *<average Kbps> <burst KB> <peak Kbps>*`]`
Adds a port group to a distributed vSwitch. For example:
`virt vmware dpg add alpha dvSwitch 10 ishaping 10 10 10 eshaping 20 20 20`
Note: Ingress shaping and egress shaping parameters are optional.
Command Mode: Privileged EXEC

`virt vmware dpg vmac` *<vNIC MAC> <port group name>* Adds a vNIC to a distributed port group. **Command Mode**: Privileged EXEC
`virt vmware dpg update` *<port group name> <dvSwitch name> <VLAN number>* `[ishaping|eshaping` *<average Kbps> <burst KB> <peak Kbps>*`]` `[ishaping|eshaping` *<average Kbps> <burst KB> <peak Kbps>*`]` Updates the parameters of a distributed port group. **Note**: Ingress shaping and egress shaping parameters are optional. **Command Mode**: Privileged EXEC
`virt vmware dpg del` *<port group name> <dvSwitch name>* Deletes a port group from a distributed vSwitch. **Command Mode**: Privileged EXEC

Feature on Demand Key Options

Use the license key to upgrade the port mode. Base port mode is the default. To upgrade the port mode, you must obtain a software license key.

After selecting a port mode, you must reset the switch for the change to take affect. Use the following command to verify the port configuration:
`show interface information`

Table 359. Feature on Demand Key Options

Command Syntax and Usage
`fod-key` Enter Feature on Demand Key mode. **Command mode:** Privileged EXEC
`enakey address` <*hostname or IP address*> `keyfile` <*file name*> `protocol tftp|sftp` Allows you to unlock the software port expansion feature. You are prompted to enter the host name or IP address of the server where the license key is stored, and the license key file name, as follows: – `46Port` – `64Port` **Note**: You must upgrade to `46Port` port mode before you can upgrade to `64Port` port mode. **Command mode:** Feature on Demand Key mode
`rmkey key` <*feature name*> Removes the specified software feature. **Command mode:** Feature on Demand Key mode
`ptkey address` <*hostname or IP address*> `key` <*feature name*> `protocol tftp|sftp file` <*file name*> Loads the specified key file to a server. **Command mode:** Feature on Demand Key mode
`invkeys address` <*hostname or IP address*> `invfile` <*file name*> `protocol tftp|sftp` Loads key code inventory information to a server. **Command mode:** Feature on Demand Key mode

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 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

This feature allows you to schedule a reboot to occur at a particular time in the 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 currently set reboot schedule.

Table 360. Boot Scheduling Options

Command Syntax and Usage
`boot schedule` <*day of week*> <*time of day*> Defines the reboot schedule. Enter the day of the week, followed by the time of day (in hh:mm format). For example: `boot schedule monday 11:30` **Command mode:** Global configuration
`no boot schedule` Cancels the next pending scheduled reboot. **Command mode:** Global configuration
`show boot` Displays the current reboot scheduling parameters. **Command mode:** All

Netboot Configuration

Netboot allows the switch to automatically download its configuration file over the network during switch reboot, and apply the new configuration. Upon reboot, the switch includes the following options in its DHCP requests:

- Option 66 (TFTP server address)
- Option 67 (file path)

If the DHCP server returns the information, the switch initiates a TFTP file transfer, and loads the configuration file into the active configuration block. As the switch boots up, it applies the new configuration file. Note that the option 66 TFTP server address must be specified in IP-address format (host name is not supported).

If DHCP is not enabled, or the DHCP server does not return the required information, the switch uses the manually-configured TFTP server address and file path.

Table 361. Netboot Options (/boot/netboot)

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

QSFP+ Port Configuration

Quad Small Form-factor Pluggable Plus (QSFP+) ports are designed to handle high-intensity traffic. Use the following commands to configure QSFP+ ports.

Table 362. QSFP+ Port Options (/boot/qsfp-40Gports)

Command Syntax and Usage
`[no] boot qsfp-40Gports` <*EXT15, EXT19*> Enables or disables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports. You must reboot the switch for this change to take effect. **Command mode:** Global configuration
`show boot qsfp-port-modes` Displays the current QSFP+ port settings. **Command mode:** All

Updating the Switch Software Image

The switch software image is the executable code running on the CN4093 10Gb Converged Scalable Switch. 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. To get the latest version of software available for your CN4093, go to:

http://www.ibm.com/support

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 FTP or TFTP server on your network
- Transferring the new image from the 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 FTP/TFTP server on your network
- The hostname or IP address of the 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} {image1|image2|boot-image} [extm-port|
mgt-port|data-port]
```

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <IP address or hostname>
```

3. 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 FTP or TFTP directory (usually `tftpboot`).

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. 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 FTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
Router# copy {image1|image2|boot-image} {ftp|tftp} [extm-port|
mgt-port|data-port]
```

   Select a port, or press <Enter> to use the default (management port).

2. Enter the name or the IP address of the FTP or TFTP server:

```
Address or name of remote host: <IP address or hostname>
```

3. Enter the name of the file into which the image will be uploaded on the FTP or TFTP server:

```
Destination file name: <filename>
```

4. Enter your username and password for the server, if applicable.

```
User name: {<username>|<Enter>}
```

5. The system then requests confirmation of what you have entered. To have the file uploaded, enter `Y`.

```
image2 currently contains Software Version 7.5.0
 that was downloaded at 0:23:39 Thu Jan  4, 2012.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 192.1.1.1. over the MGT port.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the CN4093 10Gb Converged Scalable Switch, 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 CN4093 10Gb Converged Scalable Switch 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 CN4093 10Gb Converged Scalable Switch 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) ?
```

Accessing the Menu-based CLI

To access the menu-based CLI, enter the following command from the ISCLI:

```
Router(config)# boot cli-mode ibmnos-cli
```

The default command-line interface for the CN4093 is the menu-based CLI. To access the ISCLI, enter the following command and reset the CN4093:

```
Main# boot/mode iscli
```

Users can select the CLI mode upon login, if the following ISCLI command is enabled:

```
Router(config)# boot cli-mode prompt
```

Only an administrator connected through the CLI can view and enable the `prompt` command. When `prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

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 ..............................

1 - Change booting image
2 - Change configuration block
3 - Boot in recovery mode (tftp and xmodem download of images to
    recover switch)
4 - Xmodem download (for boot image only - use recovery mode for
    application images)
5 - Reboot
6 - Exit

Please choose your menu option: 3
```

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 perform a software image recovery, press 3 and follow the screen prompts.
- To perform an Xmodem download (boot image only), press 4 and follow the screen prompts.
- To exit the Boot Management menu, press 6. The booting process continues.

Recovering from a Failed Software 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 **Boot in recovery mode**. You will see the following display:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

   – If you choose option **x** (Xmodem serial download), go to step 5.
   – If you choose option **t** (TFTP download), go to step 6.

5. **Xmodem download**: When you see the following message, change the Serial Port characteristics to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

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

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

   c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

   d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

6. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter
'q' to quit):
IP addr    :
Server addr:
Netmask    :
Gateway    :
Image Filename:
```

a. Enter the required information and press <**Enter**>.

b. You will see a display similar to the following:

```
        Host IP    : 10.10.98.110
        Server IP  : 10.10.98.100
        Netmask    : 255.255.255.0
        Broadcast  : 10.10.98.255
        Gateway    : 10.10.98.254
Installing image 6.8.3_OS.img from TFTP server 10.10.98.100
```

c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

7. Image recovery is complete. Perform one of the following steps:
   – Press **r** to reboot the switch.
   – Press **e** to exit the Boot Management menu
   – Press the Escape key (<**Esc>**) to re-display the Boot Management menu.

Recovering a Failed Boot Image

Use the following procedure to recover from a failed boot image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, 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 **4** for **Xmodem download**. You will see the following display:

```
Perform xmodem download

To download an image use 1K Xmodem at 115200 bps.
```

5. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

   a. Press <**Enter**> to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start Xmodem on your terminal emulator.You will see a display similar to the following:

```
Extracting images ... Do *NOT* power cycle the switch.
**** RAMDISK ****
Un-Protected 38 sectors
Erasing Flash...
..................................... done
Erased 38 sectors
Writing to
Flash...9....8....7....6....5....4....3....2....1....done
Protected 38 sectors
**** KERNEL ****
Un-Protected 24 sectors
Erasing Flash...
....................... done
Erased 24 sectors
Writing to Flash...9....8....7....6....5....4....3....2....1....
```

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

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

Boot image recovery is complete.

Chapter 7. Maintenance Commands

The maintenance commands are used to manage dump information and forward database information. They also include debugging commands to help with troubleshooting.

Dump information contains internal switch state data that is written to flash memory on the CN4093 10Gb Converged Scalable Switch 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 363. General Maintenance Commands

Command Syntax and Usage
`show flash-dump-uuencode` Displays dump information in uuencoded format. For details, see page 457. **Command mode:** All
`copy flash-dump tftp` Saves the system dump information via TFTP. For details, see page 458. **Command mode:** All except User EXEC
`copy flash-dump ftp` Saves the system dump information via FTP. **Command mode:** All except User EXEC
`clear flash-dump` Clears dump information from flash memory. **Command mode:** All except User EXEC
`show tech-support [l2|l3|link|port]` Dumps all CN4093 information, statistics, and configuration. You can log the output (`tsdmp`) into a file. – `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

Table 363. General Maintenance Commands

Command Syntax and Usage
`copy tech-support tftp` Redirects the technical support dump (tsdmp) to an external TFTP server. **Command mode:** All except User EXEC
`copy tech-support ftp` Redirects the technical support dump (tsdmp) to an external FTP server. **Command mode:** All except User EXEC

Forwarding Database Maintenance

The Forwarding Database commands can be used to view information and to delete a MAC address from the forwarding database or to clear the entire forwarding database. This is helpful in identifying problems associated with MAC address learning and packet forwarding decisions.

Table 364. FDB Manipulation Commands

Command Syntax and Usage
`show mac-address-table address` *<MAC address>* Displays a single database entry by its MAC address. If not specified, you are prompted for the MAC address of the device. 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 except User EXEC
`show mac-address-table interface port` *<port number or alias>* Displays all FDB entries for a particular port. **Command mode:** All except User EXEC
`show mac-address-table portchannel` *<trunk group number>* Displays all FDB entries for a particular trunk group. **Command mode:** All
`show mac-address-table vlan` *<VLAN number>* Displays all FDB entries on a single VLAN. **Command mode:** All except User EXEC
`show mac-address-table state {forward|trunk|unknown}` Displays all FDB entries of a particular state. **Command mode:** All except User EXEC
`show mac-address-table static` Displays static entries in the FBD. **Command mode:** All except User EXEC

Table 364. FDB Manipulation Commands

Command Syntax and Usage
`no mac-address-table static {`*<MAC address>*`|all}` Removes static FDB entries. **Command mode:** All except User EXEC
`no mac-address-table multicast {`*<MAC address>*`|all}` Removes static multicast FDB entries. **Command mode:** All except User EXEC
`no mac-address-table static` Clears all static entries from the Forwarding Database. **Command mode:** All except User EXEC
`clear mac-address-table` Clears the entire Forwarding Database from switch memory. **Command mode:** All except User 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

Note: IBM Networking OS debug commands are intended for advanced users. Use debug commands with caution as they can disrupt the operation of the switch under high load conditions. When debug is running under high load conditions, the CLI prompt may appear unresponsive. Before debugging, check the MP utilization to verify there is sufficient processing capacity available to perform the debug operation.

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 365. Miscellaneous Debug Commands

Command Syntax and Usage
`debug debug-flags` This command sets the flags that are used for debugging purposes. **Command mode:** Privileged EXEC

Table 365. Miscellaneous Debug Commands

Command Syntax and Usage

`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, 2012; 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 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

DCBX Maintenance

Table 366. DCBX Maintenance Options

Command Syntax and Usage
`show dcbx transmit` *<port alias or number>* Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV.
`show dcbx receive` *<port alias or number>* Displays the Type-Length-Value (TLV) list received in the DCBX TLV.

ARP Cache Maintenance

Table 367. Address Resolution Protocol Maintenance Commands

Command Syntax and Usage
`show ip arp find` *<IP address>* Shows a single ARP entry by IP address. **Command mode:** All except User EXEC
`show ip arp interface port` *<port number or alias>* Shows ARP entries on selected ports. **Command mode:** All except User EXEC
`show ip arp vlan` *<VLAN number>* Shows ARP entries on a single VLAN. **Command mode:** All except User EXEC
`show ip arp reply` Shows the list of IP addresses which the switch will respond to for ARP requests. **Command mode:** All except User EXEC
`show ip arp` Shows all ARP entries. **Command mode:** All except User EXEC
`clear arp` Clears the entire ARP list from switch memory. **Command mode:** All except User EXEC

Note: To display all or a portion of ARP entries currently held in the switch, you can also refer to “ARP Information” on page 56.

IP Route Manipulation

Table 368. IP Route Manipulation Commands

Command Syntax and Usage
`show ip route address` *<IP address>* Shows a single route by destination IP address. **Command mode:** All except User EXEC
`show ip route gateway` *<IP address>* Shows routes to a default gateway. **Command mode:** All except User EXEC
`show ip route type {indirect|direct|local|broadcast|martian|multicast}` Shows routes of a single type. **Command mode:** All except User EXEC For a description of IP routing types, see Table 37 on page 55
`show ip route tag {fixed|static|address|rip|ospf|bgp|broadcast|martian|multicast}` Shows routes of a single tag. **Command mode:** All except User EXEC For a description of IP routing tags, see Table 38 on page 56
`show ip route interface` *<IP interface>* Shows routes on a single interface. **Command mode:** All except User EXEC
`show ip route` Shows all routes. **Command mode:** All except User EXEC
`clear ip route` Clears the route table from switch memory. **Command mode:** All except User EXEC

Note: To display all routes, you can also refer to "IP Routing Information" on page 54.

LLDP Cache Manipulation

Table 369 describes the LLDP cache manipulation commands.

Table 369. LLDP Cache Manipulation commands

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` Displays information received from LLDP -capable devices. **Command mode:** All
`show lldp` Displays all LLDP information. **Command mode:** All
`clear lldp` Clears the LLDP cache. **Command mode:** All

IGMP Groups Maintenance

Table 370 describes the IGMP group maintenance commands.

Table 370. IGMP Multicast Group Maintenance Commands

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

Table 370. IGMP Multicast Group Maintenance Commands (continued)

Command Syntax and Usage
`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:** All except User EXEC

IGMP Multicast Routers Maintenance

The following table describes the maintenance commands for IGMP multicast routers (Mrouters).

Table 371. 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` Displays information for all Mrouters. **Command mode:** All
`clear ip igmp mrouter` Clears the IGMP Mrouter port table. **Command mode:** All except User EXEC

MLD Multicast Group Manipulation

Table 372 describes the Multicast Listener Discovery (MLD) manipulation options.

Table 372. MLD Maintenance

Command Syntax and Usage
`show ipv6 mld groups` Shows all MLD groups. **Command mode:** All
`show ipv6 mld interface` <*interface number*> Shows MLD groups on the specified interface. **Command mode:** All
`clear ipv6 mld mrouter` Clears all dynamic MLD multicast router group tables. **Command mode:** All except User EXEC
`clear ipv6 mld groups` Clears all dynamic MLD registered group tables. **Command mode:** All except User EXEC
`clear ipv6 mld dynamic` Clears all dynamic MLD group tables. **Command mode:** All except User EXEC

IPv6 Neighbor Discovery Cache Manipulation

Table 373 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 373. IPv6 Neighbor Discovery cache manipulation commands

Command Syntax and Usage
`show ipv6 neighbors find` *<IPv6 address>* Shows a single IPv6 Neighbor Discovery cache entry by IP address. **Command mode:** All
`show ipv6 neighbors interface port` *<port number or alias>* Shows IPv6 Neighbor Discovery cache entries on a single port. **Command mode:** All
`show ipv6 neighbors vlan` *<VLAN number>* Shows IPv6 Neighbor Discovery cache entries on a single VLAN. **Command mode:** All
`show ipv6 neighbors static` Shows static IPv6 Neighbor Discovery cache entries. **Command mode:** All
`show ipv6 neighbors` Shows all IPv6 Neighbor Discovery cache entries. **Command mode:** All
`clear ipv6 neighbors` Clears all IPv6 Neighbor Discovery cache entries from switch memory. **Command mode:** All except User EXEC

IPv6 Route Maintenance

Table 374 describes the IPv6 route maintenance commands.

Table 374. 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

Table 374. IPv6 Route Maintenance Options (continued)

Command Syntax and Usage
`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 458.

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 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 [data-port|extm-port|mgt-port] <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 FTP, enter:

```
Router# copy flash-dump ftp [data-port|extm-port|mgt-port] <server filename>
```

You are prompted for the FTP server IP 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, 2012. 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. 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 Flex System 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, Flex System 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

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document. Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A0153039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.”

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)”. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI–A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 00D2328

Printed in USA

(IP) P/N: 00D2328