Lenovo Flex System CN4093 10Gb Converged Scalable Switch

ISCLI—Industry Standard CLI Command Reference

For Networking OS 8.2

lenovo

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

First Edition (April 2015)

Contents

Preface

The *Lenovo Flex System Fabric CN4093 10Gb Converged Scalable Switch ISCLI Command Reference* describes how to configure and use the Lenovo N/OS 8.2 software with your Lenovo Flex System CN4093 10Gb Converged Scalable Switch (referred to as CN4093 throughout this document). This guide lists each command, together with the complete syntax and a functional description, from the IS Command Line Interface (ISCLI).

For documentation on installing the switches physically, see the *Installation Guide* for your CN4093. For details about the configuration and operation of the CN4093, see the *Lenovo N/OS 8.2 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 Spanning Tree Protocol and SNMP configuration parameters.

How This Book Is Organized

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

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

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

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

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

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

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

Appendix A, "Lenovo N/OS System Log Messages," lists Lenovo N/OS System Log Messages.

Appendix B, "Getting help and technical assistance," contains information on how to get help, service, technical assistance, o more information about Lenovo products.

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

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

Typographic Conventions

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

Table 1. *Typographic Conventions*

Typeface or Symbol	Meaning
`plain fixed-width text`	This type is used for names of commands, files, and directories used within the text. For example: View the `readme.txt` file. It also depicts on-screen computer output and prompts.
`bold fixed-width text`	This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example: **`show sys-info`**
bold body text	This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
italicized body text	This italicized type indicates book titles, special terms, or words to be emphasized.
angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping`** *<IP address>* you enter **`ping 192.32.10.12`**
braces **{}**	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`show portchannel {`***<1-128>***`|hash|information}`** you enter: **`show portchannel`** *<1-128>* 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 interface ip [***<1-128>***]** you enter **show interface ip** or **show interface ip** *<1-128>*
vertical line **|**	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show portchannel {***<1-128>***|hash|information}** you must enter: **show portchannel** *<1-128>* or **show portchannel hash** or **show portchannel information**

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.

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 1. This mode can be accessed using the following command: **`configure terminal`**

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

Table 1 lists the ISCLI command modes.

Table 1. *ISCLI Command Modes*

Command Mode/Prompt	Command used to enter or exit
User EXEC `CN 4093>`	Default mode, entered automatically on console Exit: **`exit`** or **`logout`**
Privileged EXEC `CN 4093#`	Enter Privileged EXEC mode, from User EXEC mode: **`enable`** Exit to User EXEC mode: **`disable`** Quit ISCLI: **`exit`** or **`logout`**
Global Configuration `CN 4093(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: **`configure terminal`** Exit to Privileged EXEC: **`end`** or **`exit`**
Interface IP `CN 4093(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: **`interface ip`** *<interface number>* Internal Management IP interface is reachable only by Management Module. Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 1. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
Interface Loopback `CN 4093(config-ip-loopback)#`	Enter Interface Loopback Configuration mode, from Global Configuration mode: **`interface loopback`** *<1-5>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Interface Port `CN 4093(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 `CN 4093(config-PortChannel)#`	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: **`interface portchannel {`***<trunk number>***`|lacp`** *<key>***`}`** Exit to Privileged EXEC mode: **`exit`** Exit to Global Configuration mode: **`end`**
VLAN `CN 4093(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 `CN 4093(config-router-ospf)#`	Enter OSPF Configuration mode, from Global Configuration mode: **`router ospf`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router OSPFv3 `CN 4093(config-router-ospf3)#`	Enter OSPFv3 Configuration mode, from Global Configuration mode: **`ipv6 router ospf`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
Router BGP `CN 4093(config-router-bgp)#`	Enter BGP Configuration mode, from Global Configuration mode: **`router bgp`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 1. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
Router RIP `CN 4093(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 `CN 4093(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 `CN 4093(config-vrrp)#`	Enter VRRP Configuration mode, from Global Configuration mode: **`router vrrp`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
IKEv2 Proposal `CN 4093(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 `CN 4093(config-router-mld)#`	Enter Multicast Listener Discovery Protocol Configuration mode, from Global Configuration mode: **`ipv6 mld`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
MST Configuration `CN 4093(config-mst)#`	Enter Multiple Spanning Tree Protocol Configuration mode, from Global Configuration mode: **`spanning-tree mst configuration`** Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
VSI Database `CN 4093(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`**

Table 1. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
EVB Profile `CN 4093(conf-evbprof)#`	Enter Edge Virtual Bridging Profile Configuration mode, from Global Configuration mode: **`virt evb profile`** *<1-16>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
UFP Virtual Port Configuration `CN 4093(config_ufp_vport)#`	Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: **`ufp port`** *<port no.>* **`vport`** *<1-4>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
SPAR Configuration `CN 4093(config-spar)#`	Enter Switch Partition Configuration mode, from Global Configuration mode: **`spar`** *<1-8>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**
FC Port Configuration `CN 4093(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 `CN 4093(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 `CN 4093(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 2. *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: o **-n**: Sets the number of attempts (optional). o **-w**: Sets the number of milliseconds between attempts (optional). o **-l**: Sets the ping request payload size (optional). o **-s**: Sets the IP source address for the IP packet (optional). o **-v**: Sets the Type Of Service bits in the IP header. o **-f**: Sets the *don't fragment* bit in the IP header (only for IPv4 addresses). o **-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 2. *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 (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:

```
CN 4093(config)#show mac-address-table interface port 12
```

or:

```
CN 4093(config)#sh ma i p 12
```

Tab Completion

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

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 or 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 3. *User Access Levels*

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	
Operator	The Operator can make temporary changes that are lost when the switch is rebooted/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, 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 4. *Information Commands*

Command Syntax and Usage
`show interface status` *<port alias or number>* Displays configuration information about the selected port(s), including: o Port alias and number o Port speed o Duplex mode (half, full, or auto) o Flow control for transmit and receive (no, yes, or both) o Link status (up, down, or disabled) For details, see page 143. **Command mode:** All
`show interface trunk` *<port alias or number>* Displays port status information, including: o Port alias and number o Whether the port uses VLAN Tagging or not o Port VLAN ID (PVID) o Port name o VLAN membership o FDB Learning status o Flooding status For details, see page 144. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each external port. For details, see page 146. **Command mode:** All
`show software-key` Displays the enabled software features. **Command mode:** All

Table 4. *Information Commands (continued)*

Command Syntax and Usage
`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 5 on page 33, with pointers to where detailed information can be found.

Table 5. *System Information Commands*

Command Syntax and Usage
show sys-info Displays system information, including: o System date and time o Switch model name and number o Switch name and location o Time of last boot o MAC address of the switch management processor o IP address of management interface o Hardware version and part number o Software image file and version number o Configuration name o Log-in banner, if one is configured o Internal temperatures For details, see page 45. **Command mode:** All
show logging [severity *<0-7>***] [reverse]** Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the **show logging messages** command. For details, see page 47. **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 6. *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 current `line console length` setting. For details, see page 284. **Command mode:** All
`show line vty length` Displays the current `line vty length` setting. For details, see page 284. **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 7. *Error Disable Information Commands*

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

SNMPv3 System Information

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

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

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

Table 8. *SNMPv3 Commands*

Command Syntax and Usage
`show snmp-server v3 user` Displays User Security Model (USM) table information. To view the table, see page 37. **Command mode:** All
`show snmp-server v3 view` Displays information about view, subtrees, mask and type of view. To view a sample, see page 38. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 39. **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 40. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 40. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 41. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 42. **Command mode:** All

Table 8. *SNMPv3 Commands (continued)*

Command Syntax and Usage
show snmp-server v3 notify Displays the Notify table information. To view a sample, see page 43. **Command mode:** All
show snmp-server v3 Displays all the SNMPv3 information. To view a sample, see page 44. **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 9. *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. Lenovo N/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                                    included
v1v2only             1                                    included
v1v2only             1.3.6.1.6.3.15                       excluded
v1v2only             1.3.6.1.6.3.16                       excluded
v1v2only             1.3.6.1.6.3.18                       excluded
```

Table 10. *SNMPv3 View Table Information Parameters*

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

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

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

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

The following command displays SNMPv3 access information:

`show snmp-server v3 access`

Command mode: All

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

Table 11. *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
usm          adminshaaes                     admingrp
```

Table 12. *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 13. *SNMPv3 Community Table Information Parameters*

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

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

`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 14. *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 15. *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 16. *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                                 included
v1v2only             1                                 included
v1v2only             1.3.6.1.6.3.15                    excluded
v1v2only             1.3.6.1.6.3.16                    excluded
v1v2only             1.3.6.1.6.3.18                    excluded

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

snmpCommunity Table:
Index      Name       User Name            Tag
---------- ---------- -------------------- ----------
snmpNotify Table:
Name                 Tag
-------------------- --------------------
snmpTargetAddr Table:
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
snmpTargetParams Table:
Name                 MP Model User Name           Sec Model Sec Level
-------------------- -------- ------------------  --------- -------
```

General System Information

The following command displays system information:

`show sys-info`

Command mode: All

```
System Information at 13:15:04 Tue Mar 17, 2015
Time zone: No timezone configured
Daylight Savings Time Status: Disabled

Lenovo Flex System Fabric CN4093 10Gb Converged Scalable Switch

Switch has been up for 0 days, 0 hours, 53 minutes and 20 seconds.
Last boot: 12:26:24 Tue Mar 17, 2015 (reset from console)

MAC address: 74:99:75:8a:94:00    IP (If 1) address: 0.0.0.0
Internal Management Port MAC Address: 74:99:75:8a:94:ef
Internal Management Port IP Address (if 128): 10.241.9.130
External Management Port MAC Address: 74:99:75:8a:94:fe
External Management Port IP Address (if 127):

Software Version 8.2.1 (FLASH image2), active configuration.
Boot kernel version 8.2.1



Chassis MTM                : 8721A1G
Chassis Serial Num         : 06MBGH4
Hardware Part Number       : 00FM512
Hardware Revision          : 05
Serial Number              : Y010CM319030
Manufacturing Date (WWYY)  : 1113
PCBA Part Number           : BAC-00107-01
PCBA Revision              : 0
PCBA Number                : 00
Board Revision             : 05
PLD Firmware Version       : 0.14

Temperature Warning        : 45 C (Warning  at 70 C / Recover at 65 C)
Temperature Shutdown       : 44 C (Shutdown at 82 C / Recover at 77 C)
Temperature Inlet          : 34 C
Temperature Exhaust        : 44 C
Temperature Asic Max       : 50 C (Warning at 100 C / Shutdown at 108 C)
Temperature FCM  Max       : 54 C

Power Consumption          : 102.960 W (12.232 V   8.417 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
- Internal temperatures

Show Software Version Brief

Table 17 lists commands used for displaying specific entries from the general system information screen.

Table 17. *Specific System Information Options*

Command Syntax and Usage
`show version brief` Displays the software version number, image file, and configuration name. **Command mode:** All

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

```
Software Version 8.2.1 (FLASH image2), active configuration.
```

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

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

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


Date    Time      Criticality level       Message
Jul  8  17:25:41    NOTICE       system: link up on port INT1
Jul  8  17:25:41    NOTICE       system: link up on port INT8
Jul  8  17:25:41    NOTICE       system: link up on port INT7
Jul  8  17:25:41    NOTICE       system: link up on port INT2
Jul  8  17:25:41    NOTICE       system: link up on port INT1
Jul  8  17:25:41    NOTICE       system: link up on port INT4
Jul  8  17:25:41    NOTICE       system: link up on port INT3
Jul  8  17:25:41    NOTICE       system: link up on port INT6
Jul  8  17:25:41    NOTICE       system: link up on port INT5
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 INT3
Jul  8  17:25:42    NOTICE       system: link up on port INT2
Jul  8  17:25:42    NOTICE       system: link up on port INT4
Jul  8  17:25:42    NOTICE       system: link up on port INT3
Jul  8  17:25:42    NOTICE       system: link up on port INT6
```

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 for which the administrator is being notified.

- `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.

Show Security Audit Log Messages

The following commands display security audit log messages:

Table 18. *Security Audit Log Information Commands*

Command Syntax and Usage
show sal [reverse] Displays the most recent security audit log messages. The reverse option displays the output in reverse order, from the newest entry to the oldest. **Command mode:** All except User EXEC
show sal sequence *<sequence number or range>* Displays the security audit log messages associated with the specified sequence number or range. **Command mode:** All except User EXEC
show sal severity *<1-6>* **[reverse]** Displays only the security audit log messages with a specific severity level between 1 and 6, from FATAL to INFORMATION correspondingly. The reverse option displays the output in reverse order, from the newest entry to the oldest. **Command mode:** All except User EXEC

Note: Security Audit Log commands are not available in Stacking mode.

Command sample output for show sal:

```
2014 Jul 16 12:40:39 2000:30:0:0:0:0:2:95 000004DC 0x00000004 Warning
1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP:
New Management IP Address 10.30.2.95 configured

2014 Jul 16 12:40:39 2000:30:0:0:0:0:2:95 000004DD 0x00000004 Warning
1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP:
New Management Gateway 10.30.1.1 configured

2014 Jul 16 12:42:40 2000:30:0:0:0:0:2:95 000004DE 0x00000004 Warning
1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP:
New Management IP Address 10.30.2.95 configured

2014 Jul 16 12:42:40 2000:30:0:0:0:0:2:95 000004DF 0x00000004 Warning
1B33D6C833832DA17E020817F40A2000 2EBBCC63AF754E04A21449CE49BFF70A 4 : IP:
New Management Gateway 10.30.1.1 configured
```

Each security audit log message has a severity level associated with it, included in text form as a prefix to the log message. One of six different prefixes is used, depending on the condition for which the administrator is being notified.

- FATAL Indicates the system is unusable
- CRITICAL Indicates critical conditions
- MAJOR Indicates action should be taken immediately
- MINOR Indicates error conditions or errored operations
- WARNING Indicates warning conditions
- INFORMATION Indicates an information message

User Status

The following command displays user status information:

`show access user`

Command mode: All except User EXEC

```
Usernames:
  user     - disabled   - offline
  oper     - disabled   - offline
  admin    - enabled    - online     1 session.
Current User ID table:
  1: name USERID  , ena, cos admin   , password valid, offline

Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

Stacking Information

Table 19 lists the Stacking information options.

Table 19. *Stacking Information Commands*

Command Syntax and Usage
show stack switch Displays information about each switch in the stack, including: o Configured Switch Number (csnum) o Attached Switch Number (asnum) when run on master switch o MAC address o Stacking state o UUID o Bay number **Command mode:** All
show stack attached-switches Displays information about each attached switch in the stack. Available only on the master switch. **Command mode:** All
show stack link Displays link information for each switch in the stack, listed by attached switch number. **Command mode:** All
show stack name Displays the name of the stack. **Command mode:** All
show stack backup Displays the unit number of the backup switch. **Command mode:** All
show stack version Displays the firmware version number for all attached switches. **Command mode:** All
show stack path-map [csnum *<1-8>***]** Displays the path used to send known unicast packets from one switch of the stack to another. **Command mode:** All

Table 19. *Stacking Information Commands*

Command Syntax and Usage
show stack push-status Displays the status of the most recent firmware and configuration file push from the master to member switches. **Command mode:** All
show stack dynamic Displays all stacking information. **Command mode:** All

Stacking Switch Information

The following command displays Stacking switch information:

`show stack switch`

Command mode: All

```
Stack name: STK
Local switch is the master.

Local switch:
   csnum             - 1
   MAC               - 74:99:75:21:8d:00
   UUID              - 534c8ca1605846299148305adc9a1f6d
   Bay Number        - 1
   Switch Type       - 14
   Chassis Type      - 6 (Flex Enterprise)
   Switch Mode (cfg) - Master
   Priority          - 250
   Stack MAC         - 74:99:75:21:8d:1f

Master switch:
   csnum             - 1
   MAC               - 74:99:75:21:8d:00
   UUID              - 534c8ca1605846299148305adc9a1f6d
   Bay Number        - 1

Backup switch:
   csnum             - 5
   MAC               - 74:99:75:21:8c:00
   UUID              - 98c587636548429aba5010f8c62d4e27
   Bay Number        - 1

Configured Switches:
--------------------------------------------------------------------------
csnum             UUID                 Bay       MAC         asnum
--------------------------------------------------------------------------
 C1   534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  A1
 C2   534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  A3
 C3   534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  A2
 C4   534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  A4
 C5   98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  A5

Attached Switches in Stack:
--------------------------------------------------------------------------
asnum             UUID                 Bay       MAC         csnum   State
--------------------------------------------------------------------------
 A1   534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  C1  IN_STACK
 A2   534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  C3  IN_STACK
 A3   534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  C2  IN_STACK
 A4   534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  C4  IN_STACK
 A5   98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  C5  IN_STACK
```

Stack switch information includes the following:

- Stack name
- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Stack Backup
- Configured switch numbers and their associated assigned switch numbers
- Attached switch numbers and their associated configured switch numbers

Attached Switches Information

The following command displays information about attached switches, when run on master switch:

show stack attached-switches

Command mode: All

```
Attached Switches in Stack
-------------------------------------------------------------------------------
asnum            UUID                 Bay       MAC         csnum   State
-------------------------------------------------------------------------------
 A1   534c8ca1605846299148305adc9a1f6d  1  74:99:75:21:8d:00  C1  IN_STACK
 A2   534c8ca1605846299148305adc9a1f6d  3  08:17:f4:0a:2d:00  C3  IN_STACK
 A3   534c8ca1605846299148305adc9a1f6d  2  08:17:f4:84:34:00  C2  IN_STACK
 A4   534c8ca1605846299148305adc9a1f6d  4  74:99:75:1c:77:00  C4  IN_STACK
 A5   98c587636548429aba5010f8c62d4e27  1  74:99:75:21:8c:00  C5  IN_STACK
```

Stack Name Information

The following command displays the name of the stack:

show stack name

Command mode: All

```
Stack name: STK
```

Stack Backup Switch Information

The following command displays the unit number for the backup switch:

show stack backup

Command mode: All

```
Current config Backup unit number = 5
```

Stack Version Information

The following command displays firmware version information for each switch in the stack:

`show stack version`

Command mode: All

```
Switch Firmware Versions:
-------------------------------------------------
asnum  csnum        MAC           S/W        Version         Serial #
-----  -----       -----         ------  ---------------  ------------
 A1     C1   74:99:75:21:8d:00   image1  7.7.1.10         Y250CM28Y653
 A2     C3   08:17:f4:0a:2d:00   image1  7.7.1.10         US7049000Y
 A3     C2   08:17:f4:84:34:00   image1  7.7.1.10         Y010CM161680
 A4     C4   74:99:75:1c:77:00   image1  7.7.1.10         Y010CM28E857
 A5     C5   74:99:75:21:8c:00   image1  7.7.1.10         Y250CM28Y639
```

Stack Packet Path Information

The following command displays information about the path used to send known unicast packets between the switches of a stack.

`show stack path-map`

Command mode: All

```
Packet path Information:
-------------------------------------------------------------------------------
To->       Swu 1 |Swu  2 |Swu  3 |Swu  4 |Swu  5 |Swu  6 |Swu  7 |Swu  8 |
    Swu 1 |    0 |  1:45 |  1:45 |  1:49 |  1:49 |     0 |     0 |     0 |
    Swu 2 | 2:61 |     0 |  2:61 |  2:57 |  2:57 |     0 |     0 |     0 |
    Swu 3 | 3:57 |  3:61 |     0 |  3:57 |  3:61 |     0 |     0 |     0 |
    Swu 4 | 4:57 |  4:61 |  4:57 |     0 |  4:61 |     0 |     0 |     0 |
    Swu 5 | 5:45 |  5:49 |  5:49 |  5:45 |     0 |     0 |     0 |     0 |
    Swu 6 |    0 |     0 |     0 |     0 |     0 |     0 |     0 |     0 |
    Swu 7 |    0 |     0 |     0 |     0 |     0 |     0 |     0 |     0 |
    Swu 8 |    0 |     0 |     0 |     0 |     0 |     0 |     0 |     0 |
```

Stack Push Status Information

The following command displays the status of the most recent firmware and configuration file push from the master to member switches:

`show stack push-status`

Command mode: All

```
Image 1 transfer status info:
        Switch 08:17:f4:0a:2d:00:
                not received - file not sent or transfer in progress
        Switch 08:17:f4:84:34:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:1c:77:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:21:8c:00:
                not received - file not sent or transfer in progress

Image 2 transfer status info:
        Switch 08:17:f4:0a:2d:00:
                not received - file not sent or transfer in progress
        Switch 08:17:f4:84:34:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:1c:77:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:21:8c:00:
                not received - file not sent or transfer in progress

Boot image transfer status info:
        Switch 08:17:f4:0a:2d:00:
                not received - file not sent or transfer in progress
        Switch 08:17:f4:84:34:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:1c:77:00:
                not received - file not sent or transfer in progress
        Switch 74:99:75:21:8c:00:
                not received - file not sent or transfer in progress

Config file transfer status info:
        Switch 08:17:f4:0a:2d:00:
                last receive successful
        Switch 08:17:f4:84:34:00:
                last receive successful
        Switch 74:99:75:1c:77:00:
                last receive successful
        Switch 74:99:75:21:8c:00:
                last receive successful
```

Layer 2 Information

The following commands display Layer 2 information.

Table 20. *Layer 2 Information Commands*

Command Syntax and Usage
`show dot1x information` Displays 802.1X Information. For details, see page 72. **Command mode:** All
`show spanning-tree` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership. In addition to seeing if spanning tree groups (STGs) are enabled or disabled, you can view the following STG bridge information: o Priority o Hello interval o Maximum age value o Forwarding delay o Aging time You can also see the following port-specific STG information: o Port alias and priority o Cost o State For details, see page 74. **Command mode:** All
`show spanning-tree stp` *<1-128>* **`information`** Displays information about a specific Spanning Tree Group. For details, see page 79. **Command mode:** All

Table 20. *Layer 2 Information Commands (continued)*

Command Syntax and Usage
show spanning-tree mst *<0-32>* **[information]** Displays Multiple Spanning Tree Protocol (MSTP) information for the specified instance, including the MSTP digest and VLAN membership. MSTP port information includes: o Port number and priority o Cost o State o Role o Designated bridge and port o Type For details, see page 83. **Command mode:** All
show spanning-tree mst configuration Displays the current MSTP settings. **Command mode:** All
show portchannel information Displays the state of each port in the various static or LACP trunk groups. For details, see page 85. **Command mode:** All
show vlan Displays VLAN configuration information for all configured VLANs, including: o VLAN Number o VLAN Name o Status o Port membership of the VLAN For details, see page 86. **Command mode:** All
show failover trigger [*<trigger number>***|information]** Displays Layer 2 Failover information. For details, see page 63. **Command mode:** All

Table 20. *Layer 2 Information Commands (continued)*

Command Syntax and Usage
`show hotlinks information` Displays Hot Links information. For details, see page 65. **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 128K MAC address entries on the MP per switch.

Table 21. *FDB Information Commands*

Command Syntax and Usage
show mac-address-table Displays all entries in the Forwarding Database. **Command mode:** All For more information, see page 60.
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 all Displays both unicast (static and dynamic) and multicast (static) entries in the Forwarding Database. **Command mode:** All
show mac-address-table configured static Displays all configured static MAC entries in the FDB. **Command mode:** All
show mac-address-table interface port *<port alias or number>* Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table multicast Displays all Multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table portchannel *<trunk group number>* Displays all FDB entries for a particular trunk group (portchannel). **Command mode:** All
show mac-address-table private-vlan *<VLAN number>* Displays all FDB entries on a single private VLAN. **Command mode:** All

Table 21. *FDB Information Commands (continued)*

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

Show All FDB Information

The following command displays Forwarding Database information:

show mac-address-table

Command mode: All

```
     MAC address     VLAN  Port  Trnk  State  Permanent
  -----------------  ----  ----  ----  -----  ---------
  00:04:38:90:54:18     1  EXT4         FWD
  00:09:6b:9b:01:5f     1  INT13        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 that reference the address as a destination will be listed under "Reference ports".

Show FDB Multicast Address Information

The following commands display Multicast Forwarding Database information:

Table 22. *Multicast FDB Information Commands*

Command Syntax and Usage
show mac-address-table multicast Displays all Multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table multicast address *<MAC address>* Displays a single FDB multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `03:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `030020123456`. **Command mode:** All
show mac-address-table multicast interface port *<port alias or number>* Displays all FDB multicast entries for a particular port. **Command mode:** All
show mac-address-table multicast vlan *<VLAN number>* Displays all FDB multicast entries on a single VLAN. **Command mode:** All

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to "Forwarding Database Maintenance" on page 589.

Link Aggregation Control Protocol Information

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

Table 23. *LACP Information Commands*

Command Syntax and Usage
show lacp aggregator *<aggregator ID>* Displays detailed information about the LACP aggregator. **Command mode:** All
show lacp information Displays a summary of LACP information. For details, see page 62. **Command mode:** All
show interface port *<port alias or number>* **lacp information** Displays LACP information about the selected port. **Command mode:** All

Link Aggregation Control Protocol

The following command displays LACP information:

show lacp information

Command mode: All

```
port    mode    adminkey  operkey    selected    prio  aggr  trunk  status  minlinks
--------------------------------------------------------------------------------
1       active      1000     1000   individual  32768    --     --   down       1
2       active      2000     2000    suspended  32768    --     --   down       1
3       active      3000     2000       yes     32768     1    65*    up        1
4       active      3000     2000    suspended  32768    --    65*   down       1
...
(*) LACP PortChannel is statically bound to the admin key
```

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, down or standby).
- `minlinks` Displays the minimum number of active links in the LACP trunk.

Layer 2 Failover Information Commands

The following command displays Layer 2 Failover information:

Table 24. *Layer 2 Failover Information Commands*

Command Syntax and Usage
`show failover trigger` *<trigger number>* **`[information]`** Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All
`show failover trigger [information]` Displays a summary of Layer 2 Failover information. For details, see page 63. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

`show failover trigger`

Command mode: All

```
trunk 1
 EXT2       Operational
 EXT3       Operational

Control State: Auto Disabled
Member      Status
---------   -----------
 INT1       Operational
 INT2       Operational
 INT3       Operational
 INT4       Operational

Trigger 2 Manual Monitor: Enabled
Trigger 2 limit: 0
Monitor State: Down
Member      Status
---------   -----------
adminkey 62
 EXT20      Failed
Control State: Auto Disabled
Member      Status
---------   -----------
Physical ports
 INTC1      Failed
Virtual  ports
 INTB1.2    Failed
 INTB2.2    Failed
 INTB3.2    Failed
 INTB4.2    Failed
 INTB5.2    Failed
...
```

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

- Port link is up.
- If Spanning-Tree is enabled, the port is in the `Forwarding` state.
- If the port is a member of an LACP trunk group, the port is aggregated.

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

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

A control port's status is displayed as `Failed` when the monitor trigger state is `Down` or when the controlled port is a vPort which is not properly configured (UFP feature is not enabled in switch, port is not configured as UFP port, vport is not enabled or physical port is not enabled).

Hot Links Information

The following command displays Hot Links information:

`show hotlinks information`

Command mode: All

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
Hot Links BPDU flood: disabled
Hot Links FDB update: disabled
FDB update rate (pps): 500

Current Trigger 12 setting: enabled
name "TG-12", preempt enabled, fdelay 30 sec

Active state: None

Master settings:
        port EXT2
Backup settings:
        port EXT3
```

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

The following commands display Edge Control Protocol (ECP) information.

Table 25. *ECP Information Options*

Command Syntax and Usage
show ecp channels Displays all Edge Control Protocol (ECP) channels. **Command mode:** All
show ecp retransmit-interval Displays Edge Control Protocol (ECP) retransmit interval. **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 26. *LLDP Information Commands*

Command Syntax and Usage
show lldp [information] Displays LLDP information. **Command mode:** All
show lldp port [*<port number or range>***]** Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
show lldp port *<1-16>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information. **Command mode:** All
show lldp port *<1-16>* **vport** *<1-4>* **tlv evb** Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specifiec virtual port. **Command mode:** All
show lldp receive Displays information about the LLDP receive state machine. **Command mode:** All
show lldp remote-device [*<1-256>***|detail|** **|port [***<port number or range>***]]** Displays information received from LLDP-capable devices. To view a sample display, see page 68. **Command mode:** All
show lldp transmit Displays information about the LLDP transmit state machine. **Command mode:** All

LLDP Remote Device Information

The following command displays LLDP remote device information:

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

Command mode: All

```
LLDP Remote Devices Information
Legend(possible values in DMAC column) :
NB   - Nearest Bridge          - 01-80-C2-00-00-0E
NnTB - Nearest non-TPMR Bridge - 01-80-C2-00-00-03
NCB  - Nearest Customer Bridge - 01-80-C2-00-00-00
Total number of current entries: 1

LocalPort|Index|Remote Chassis ID|Remote Port|Remote System Name|DMAC
---------|-----|-----------------|-----------|------------------|----
EXTM     | 1   |74 99 75 df 88 00|2          |G8052-11          |NB
```

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

```
Local Port Alias: 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 : Lenovo Networking Operating System
RackSwitch G8264, Lenovo Networking OS: version 7.8.0.24,
Boot image: version 7.8.0.24

        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 27. *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

The following commands display OAM Discovery information.

Table 28. *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 29. *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
-----  ------------  ------------  --------------  ---------- --------
*INT1  force-auth    unauthorized  initialize      initialize   none
*INT2  force-auth    unauthorized  initialize      initialize   none
 INT3  force-auth    unauthorized  initialize      initialize   none
*INT4  force-auth    unauthorized  initialize      initialize   none
*INT5  force-auth    unauthorized  initialize      initialize   none
*INT6  force-auth    unauthorized  initialize      initialize   none
*INT7  force-auth    unauthorized  initialize      initialize   none
 INT8  force-auth    unauthorized  initialize      initialize   none
 INT9  force-auth    unauthorized  initialize      initialize   none
*INT10 force-auth    unauthorized  initialize      initialize   none
*INT11 force-auth    unauthorized  initialize      initialize   none
*INT12 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
*EXT11 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 Lenovo Switch that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

Table 30. *802.1X Parameter Descriptions*

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

Table 30. *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: o initialize o disconnected o connecting o authenticating o authenticated o aborting o held o forceAuth
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: o initialize o request o response o success o fail o timeout o idle

Spanning Tree Information

The following command displays Spanning Tree information:

`show spanning-tree`

Command mode: All

Note: Based on the Spanning Tree mode enabled, the command output differs:

- VLAN Rapid Spanning Tree mode (`pvrst`):

```
Pvst+ compatibility mode enabled

----------------------------------------------------------------
Spanning Tree Group 2: On (PVRST)
VLANs:  4000

Current Root:            Path-Cost  Port  Hello  MaxAge  FwdDel
8002 74:99:75:bd:b6:00        0       0     2      20      15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology Change Counts
              32770      2      20      15     300                  0

    Port    Prio    Cost    State Role Designated Bridge      Des Port Type
----------- ---- ---------- ----- ---- ---------------------- -------- -----
EXT13       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT14       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT15       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT16       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT17       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT20       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT21       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT22       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.

----------------------------------------------------------------
Spanning Tree Group 32: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
8020 74:99:75:bd:b6:00        0       0    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology Change Counts
              32800      2      20      15     300                  0

    Port    Prio    Cost    State Role Designated Bridge      Des Port Type
----------- ---- ---------- ----- ---- ---------------------- -------- -----

Note: There is no active STP port in Spanning Tree Group 32.

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

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

- Rapid Spanning Tree mode (`rstp`)

```
Pvst+ compatibility mode enabled

----------------------------------------------------------------------
Spanning Tree Group 1: On (RSTP)
VLANs:  1 4000 4095

Current Root:            Path-Cost  Port  Hello  MaxAge  FwdDel
0000 74:99:75:bd:c4:00      990    EXT15    2      20      15

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

    Port    Prio    Cost    State Role Designated Bridge      Des Port Type
----------- ---- ---------- ----- ---- --------------------- -------- -----
EXT13       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT14       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT15       128       990!+ FWD   ROOT 0000-74:99:75:bd:c4:00     8046  P2P
EXT16       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8036  P2P
EXT17       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT20       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT21       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
EXT22       128      4990!+ DISC  DESG 8002-74:99:75:bd:b6:00     8047  P2P
MGT1          0         0   FWD  *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

- Multiple Spanning Tree mode (`mstp`)

```
Pvst+ compatibility mode enabled

Mstp Digest: 0x5e5b21c3e2cb4f144cabc50e88b9bdea

Common Internal Spanning Tree:

VLANs MAPPED:  2-3999 4001-4094
VLANs:  4095

Current Root:            Path-Cost  Port  MaxAge  FwdDel
0000 74:99:75:bd:c4:00        0    EXT15    20     15

Cist Regional Root:       Path-Cost
0000 74:99:75:bd:c4:00      990

Parameters:  Priority  MaxAge  FwdDel  Hops
               4096      20      15     20
    Port    Prio    Cost    State Role Designated Bridge      Des Port Hello Type
----------- ---- ---------- ----- ---- ---------------------- -------- ----- -----
EXT13       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056     2   P2P
EXT14       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056     2   P2P
EXT15       128       990!+ FWD   ROOT 0000-74:99:75:bd:c4:00     8046     2   P2P
EXT16       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056     2   P2P
EXT17       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066     2   P2P
EXT20       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066     2   P2P
EXT21       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066     2   P2P
EXT22       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066     2   P2P
MGT1          0         0   FWD  *
* = STP turned off for this port.
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.

------------------------------------------------------------------
Spanning Tree Group 2: On (MSTP)
VLANs MAPPED:  4000
VLANs:  4000

Current Root:            Path-Cost  Port
8000 74:99:75:bd:b6:00        0       0

Parameters:  Priority  Aging  Topology Change Counts
              32768     300                  3

    Port    Prio    Cost    State Role Designated Bridge      Des Port Type
----------- ---- ---------- ----- ---- ---------------------- -------- -----
EXT13       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT14       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT15       128       990!+ FWD   ROOT 0000-74:99:75:bd:c4:00     8046   P2P
EXT16       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT17       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT20       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT21       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT22       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

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

Table 31. *CIST Parameter Descriptions*

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from discarding to learning and from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20.

The following port-specific CIST information is also displayed:

Table 32. *CIST Parameter Descriptions*

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

Table 32. *CIST 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 port ID of the port on the Designated Bridge to which this port is connected.
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.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

RSTP/PVRST Information

The following command displays RSTP/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
----- ---- --------- -----  ---- ---------------------- --------  -----
INT1     0         0  DSB *
INT2     0         0  DSB *
INT3     0         0  FWD *
INT4     0         0  DSB *
INT5     0         0  DSB *
INT6     0         0  DSB *
INT7     0         0  DSB *
INT8     0         0  DSB *
INT9     0         0  DSB *
INT10    0         0  DSB *
INT11    0         0  DSB *
INT12    0         0  DSB *
INT13    0         0  DSB *
INT14    0         0  DSB *
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
...
* = 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 unit that you are using and the firmware versions and options that are installed.

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

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

Table 33. *RSTP/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 discarding 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 34. *RSTP/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 mode can be one of the following: Discarding (`DISC`), Learning (`LRN`), Forwarding (`FWD`), or Disabled (`DSB`).

Table 34. *RSTP/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.

Spanning Tree Bridge Information

The following command displays Spanning Tree bridge information:

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

Command mode: All

```
Vlan      Priority    Hello     MaxAge    FwdDel    Protocol
------    --------    ------    ------    ------    --------
1         61440       2         20        15        PVRST
```

Table 35. *Bridge Parameter Descriptions*

Parameter	Description
VLANs	VLANs that are part of the Spanning Tree Group.
Priority	The bridge priority parameter controls which bridge on the network will become the STP root bridge. The lower the value, the higher the priority.
Hello	The hello time parameter specifies, in seconds, how often the 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 discaring to learning and from learning state to forwarding state.
Protocol	The STP protocol run by the Spanning Tree Group.

Spanning Tree Root Information

The following command displays information about the root switches in every STP group:

`show spanning-tree root`

Command mode: All

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

Table 36. *Bridge Parameter Descriptions*

Parameter	Description
Instance	Spanning Tree instance
Root ID	Indicates the root switch MAC address and port number.
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.
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 discarding to learning and from learning state to forwarding state.
Root Port	Port number allocated to the STP instance on the root switch.

Multiple Spanning Tree Information

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

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

Command mode: All

```
Mstp Digest: 0x5e5b21c3e2cb4f144cabc50e88b9bdea

------------------------------------------------------------------
Spanning Tree Group 2: On (MSTP)
VLANs MAPPED:  4000
VLANs:  4000

Current Root:            Path-Cost  Port
8000 74:99:75:bd:b6:00        0       0

Parameters:  Priority  Aging  Topology Change Counts
              32768     300                  3

    Port    Prio    Cost    State Role Designated Bridge      Des Port Type
----------- ---- ---------- ----- ---- ---------------------- -------- -----
EXT13       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT14       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT15       128       990!+ FWD   ROOT 0000-74:99:75:bd:c4:00     8046   P2P
EXT16       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8056   P2P
EXT17       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT20       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT21       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
EXT22       128       200!+ FWD   DESG 1000-74:99:75:bd:b6:00     8066   P2P
! = Automatic path cost.
+ = Portchannel cost, not the individual port cost.
```

The following port-specific MSTP information is also displayed:

Table 37. *MSTP 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 37. *MSTP 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

The following commands display VLAN information.

Table 38. *VLAN Information Commands*

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

The following command displays VLAN information:

`show vlan [`*<VLAN number>***`]`**

Command mode: All

```
VLAN        Name         Status MGT           Ports
----  ------------------ ------ --- -----------------------------------
1     Default VLAN        ena   dis  INTA1-EXT22
10    VLAN 10             ena   dis  empty
4095  Mgmt VLAN           ena   ena  EXTM MGT1

Primary  Secondary  Type             Ports
-------  ---------  ---------------  --------------------------
```

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 Lenovo Switch 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
- VLAN Name
- Status
- Management status of the VLAN
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

Layer 3 Information

The following commands display Layer 3 information.

Table 39. *Layer 3 Information Commands*

Command Syntax and Usage
show arp Displays Address Resolution Protocol (ARP) information. For details, see page 94. **Command mode:** All
show interface ip [*<interface number>***]** Displays IPv4 interface information. For details, see page 121. **Command mode:** All
show ikev2 Displays IKEv2 information. For more information options, see page 125. **Command mode:** All
show ip bgp information [*<IPv4 address>***] [***<IPv4 mask>***]** Displays Border Gateway Protocol (BGP) information. For details, see page 97. **Command mode**: All
show ip dns Displays the current Domain Name System settings. **Command mode:** All
show ip ecmp Displays ECMP static route information. For details, see page 112. **Command mode**: All
show ip gateway *<1-4>* Displays the current gateway settings. **Command mode:** All
show ip igmp Displays IGMP Information. For more IGMP information options, see page 113. **Command mode**: All
show ip information Displays all IP information. **Command mode:** All

Table 39. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
`show ip interface brief` Displays IP Information. For details, see page 124. IP information, includes: o IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. o Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status. o IP forwarding settings, network filter settings, route map settings. **Command mode:** All
`show ip ospf information` Displays OSPF information. For more OSPF information options, see page 98. **Command mode**: All
`show ip pim component [`*<1-2>***`]`** Displays Protocol Independent Multicast (PIM) component information. For more PIM information options, see page 129. **Command mode:** All
`show ip rip interface` Displays RIP user's configuration. For details, see page 107. **Command mode**: All
`show ip route` Displays all routes configured on the switch. For details, see page 92. **Command mode:** All
`show ip slp` Displays information about the Service Location Protocol (SLP) configuration. For command options, see page 155. **Command mode:** All
`show ip vrrp information` Displays VRRP information. For details, see page 120. **Command mode:** All
`show ipsec manual-policy` Displays information about manual key management policy for IP security. For more information options, see page 127. **Command mode:** All
`show ipv6 gateway6` *<1,3-4>* Displays the current IPv6 default gateway configuration. **Command mode**: All

Table 39. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
show ipv6 interface [<*interface number*>**]** Displays IPv6 interface information. For details, see page 122. **Command mode:** All
show ipv6 mld groups Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see page 118. **Command mode**: All
show ipv6 neighbors Displays IPv6 Neighbor Discovery cache information. For more information options, see page 110. **Command mode**: All
show ipv6 ospf information Displays OSPFv3 information. For more OSPFv3 information options, see page 103. **Command mode**: All
show ipv6 pmtu [<*destination IPv6 address*>**]** Displays IPv6 Path MTU information. For details, see page 123. **Command mode:** All
show ipv6 prefix Displays IPv6 Neighbor Discovery prefix information. For details, see page 111. **Command mode**: All
show ipv6 route Displays IPv6 routing information. For more information options, see page 108. **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 40. *Route Information Commands*

Command Syntax and Usage
show ip route [all] Displays all routes configured in the switch. For more information, see page 92. **Command mode:** All
show ip route address *<IP address>* Displays a single route by destination IP address. **Command mode:** All
show ip route ecmphash Displays the current ECMP hashing mechanism. **Command mode:** All
show ip route gateway *<IP address>* Displays routes to a single gateway. **Command mode:** All
show ip route interface *<interface number>* Displays routes on a single interface. **Command mode:** All
show ip route static Displays static routes configured on the switch. **Command mode:** All
show ip route tag {address|bgp|broadcast|fixed|martian| |multicast|ospf|rip|static} Displays routes of a single tag. For a description of IP routing tags, see Table 42 on page 92. **Command mode:** All
show ip route type {broadcast|direct|indirect|local| |martian|multicast} Displays routes of a single type. For a description of IP routing types, see Table 41 on page 92. **Command mode:** All

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       Metric 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 41. *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 42. *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.
address	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP).

Table 42. *IP Routing Tag Parameters (continued)*

Parameter	Description
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

ARP Information

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 44 on page 95), VLAN and port for the address, and port referencing information.

Table 43. *ARP Information Commands*

Command Syntax and Usage
show [ip] arp [all] Displays all ARP entries. including: o IP address and MAC address of each entry o Address status flag (see below) o The VLAN and port to which the address belongs o The elapsed time (in seconds) since the ARP entry was learned For more information, see page 95. **Command mode:** All
show [ip] arp find *<IP address>* Displays a single ARP entry by IP address. **Command mode:** All
show [ip] arp interface port *<port alias or number>* Displays the ARP entries on a single port. **Command mode:** All
show [ip] arp reply Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags. **Command mode:** All
show [ip] arp static Displays all static ARP entries. **Command mode:** All
show [ip] arp vlan *<VLAN number>* Displays the ARP entries on a single VLAN. **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 44. *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 Pass-Up
-------------- --------------- ----------------- ---- -------
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

The following commands display BGP information.

Table 45. *BGP Peer Information Commands*

Command Syntax and Usage
show ip bgp aggregate-address Displays BGP peer routes. See page 97 for a sample output. **Command mode:** All
show ip bgp information Displays the BGP routing table. See page 97 for a sample output. **Command mode:** All
show ip bgp neighbor information Displays BGP peer information. See page 96 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 97 for a sample output. **Command mode:** All

BGP Peer information

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

show ip bgp neighbor information

Command mode: All

```
BGP Peer Information:

  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 Aggregation Information

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

`show ip bgp aggregate-address`

Command mode: All

```
Current BGP aggregation settings:
  1: addr 4.2.0.0, mask 255.0.0.0, enabled
  2: addr 5.5.0.0, mask 255.255.0.0, enabled
```

Dump BGP Information

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

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

Command mode: All

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

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

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

OSPF Information

The following commands display OSPF information.

Table 46. *OSPF Information Commands*

Command Syntax and Usage
show ip ospf area *<0-2>* Displays area information for a particular area index. **Command mode:** All
show ip ospf area information Displays area information for all areas. **Command mode:** All
show ip ospf area-virtual-link information Displays information about all the configured virtual links. **Command mode:** All
show ip ospf general-information Displays general OSPF information. See page 99 for a sample output. **Command mode:** All
show ip ospf information Displays OSPF information. **Command mode:** All
show ip ospf interface *<interface number>* Displays OSPF information for a particular IP interface. See page 100 for a sample output. **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 100 for a sample output. **Command mode:** All
show ip ospf neighbor Displays the status of all the current neighbors. **Command mode:** All
show ip ospf routes Displays OSPF routing table. See page 105 for a sample output. **Command mode:** All

Table 46. *OSPF Information Commands (continued)*

Command Syntax and Usage
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

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 5.5.5.5, Area 0.0.0.1, Passive interface, Admin Status UP
Router ID 1.1.1.2, 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 Information Route Codes

The following command displays OSPF route information:

show ip ospf routes

Command mode: All

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

OSPF Database Information

The following commands display OSPF Database information.

Table 47. *OSPF Database Information Commands*

Command Syntax and Usage
show ip ospf database Displays all the LSAs. **Command mode:** All
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 use of this command is as follows: o `asbr-summary advertising-router 20.1.1.1` displays ASBR summary LSAs having the advertising router 20.1.1.1. o `asbr-summary link-state-id 10.1.1.1` displays ASBR summary LSAs having the link state ID 10.1.1.1. o `asbr-summary self` displays the self advertised ASBR summary LSAs. o `asbr-summary` with no parameters displays all the ASBR summary LSAs. **Command mode:** All
show ip ospf database database-summary Displays the following information about the LS database in a table format: o Number of LSAs of each type in each area. o Total number of LSAs for each area. o Total number of LSAs for each LSA type for all areas combined. o Total number of LSAs for all LSA types for all areas combined. No parameters are required. **Command mode:** All
show ip ospf database external [advertising-router *<router ID>***| |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

Table 47. *OSPF Database Information Commands (continued)*

Command Syntax and Usage
show ip ospf database nssa Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. **Command mode:** All
show ip ospf database router [advertising-router *<router ID>***||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

OSPFv3 Information

The following commands display OSPFv3 information.

Table 48. *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 area-range information Displays OSPFv3 summary ranges. **Command mode:** All
show ipv6 ospf area-virtual-link Displays information about all the configured virtual links. **Command mode:** All
show ipv6 ospf border-routers Displays OSPFv3 routes to an ABR or ASBR. **Command mode:** All
show ipv6 ospf host Displays OSPFv3 host configuration information. **Command mode:** All
show ipv6 ospf information Displays all OSPFv3 information. To view a sample display, see page 104. **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 105. **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

Table 48. *OSPFv3 Information Options*

Command Syntax and Usage
show ipv6 ospf redist-config Displays OSPFv3 redistribution information to be applied to routes learned from the route table. **Command mode:** All
show ipv6 ospf request-list *<nbr router-id (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 routes Displays OSPFv3 routing table. To view a sample display, see page 105. **Command mode:** All
show ipv6 ospf summary-prefix *<area index (0-2)>* Displays the OSPFv3 external summary-address configuration information. **Command mode:** All

OSPFv3 Information Dump

The following command displays OSPFv3 information:

show ipv6 ospf information

Command mode: All

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

OSPFv3 Interface Information

The following command displays OSPFv3 interface information:

show ipv6 ospf interface

Command mode: All

```
       Ospfv3 Interface Information

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

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

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

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

OSPFv3 Routes Information

The following command displays OSPFv3 route information:

show ipv6 ospf routes

Command mode: All

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

OSPFv3 Database Information

The following commands display OSPFv3 Database information.

Table 49. *OSPFv3 Database Information Options*

Command Syntax and Usage
show ipv6 ospf database [detail|hex] Displays all the LSAs. **Command mode:** All
show ipv6 ospf database as-external [detail|hex] Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database inter-prefix [detail|hex] Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database inter-router [detail|hex] Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database intra-prefix [detail|hex] Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database link [detail|hex] Displays Link LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database network [detail|hex] Displays Network LSAs database information. If no parameter is supplied, it displays condensed information. **Command mode:** All
show ipv6 ospf database 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

Routing Information Protocol

The following commands display Routing Information Protocol (RIP) information.

Table 50. *Routing Information Protocol Commands*

Command Syntax and Usage
show ip rip routes Displays RIP routes. For more information, see page 107. **Command mode:** All
show interface ip *<interface number>* **rip** Displays RIP user's configuration. For more information, see page 107. **Command mode:** All

RIP Routes Information

The following command displays RIP route information:

show ip rip routes

Command mode: All

```
>> IP Routing#

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

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

RIP Interface Information

The following command displays RIP user information:

show ip rip interface *<interface number>*

Command mode: All

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

IPv6 Routing Information

Table 51 describes the IPv6 Routing information options.

Table 51. *IPv6 Routing Information Commands*

Command Syntax and Usage
show ipv6 route Displays all IPv6 routing information. For more information, see page 109. **Command mode:** All
show ipv6 route address *<IPv6 address>* Displays a single route by destination IP address. **Command mode:** All
show ipv6 route gateway *<default gateway address>* Displays routes to a single gateway. **Command mode:** All
show ipv6 route interface *<interface number>* Displays routes on a single interface. **Command mode:** All
show ipv6 route static Displays all static IPv6 routes. **Command mode:** All
show ipv6 route type {connected|static|ospf} Displays routes of a single type. **Command mode:** All
show ipv6 route summary Displays a summary of IPv6 routing information, including inactive routes. **Command mode:** All

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
        D - Data Gateway from RA
        M - Management Gateway, E - Ext-Management Gateway
        N - Management Gateway from RA
        F - Ext-Management Gateway from RA

S   ::/0 [1/20]
        via 2001:2:3:4::1, Interface 2
C   2001:2:3:4::/64 [1/1]
        via ::, Interface 2
C   fe80::20f:6aff:feec:f701/128 [1/1]
        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

The following commands display IPv6 Neighbor Discovery Cache information.

Table 52. *IPv6 Neighbor Discovery Cache Information Commands*

Command Syntax and Usage
show ipv6 neighbors Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 110. **Command mode:** All
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 static Displays static IPv6 Neighbor Discovery cache entries. **Command mode:** All
show ipv6 neighbors vlan *<VLAN number>* Shows IPv6 Neighbor Discovery cache entries on a single VLAN. **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
10.20.2.2       255.255.255.255 10.234.4.4        1    up
10.20.2.2       255.255.255.255 10.235.5.5        1    up
```

ECMP 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 ecmphash

Command mode: All

```
ECMP Hash Mechanism: dipsip
```

IGMP Information

The following commands display IGMP information:

Table 53. *IGMP Information Commands*

Command Syntax and Usage
show ip igmp Displays the current IGMP configuration parameters. **Command mode:** All
show ip igmp filtering Displays current IGMP Filtering parameters. **Command mode:** All
show ip igmp groups Displays information for all multicast groups. For a command sample output, see page 116. **Command mode:** All
show ip igmp groups address *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
show ip igmp groups detail *<IP address>* Displays details about an IGMP multicast group, including source and timer information. **Command mode:** All
show ip igmp groups interface port *<port alias or number>* Displays all IGMP multicast groups on a single port. **Command mode:** All
show ip igmp groups portchannel *<trunk number>* Displays all IGMP multicast groups on a single trunk group. **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 ipmcgrp Displays information for all IPMC groups. For details, see page 117. **Command mode:** All
show ip igmp mrouter [information] Displays IGMP Multicast Router information. For details, see page 117. **Command mode:** All

Table 53. *IGMP Information Commands (continued)*

Command Syntax and Usage
show ip igmp mrouter dynamic Displays IGMP Multicast Router dynamic information. **Command mode:** All
show ip igmp mrouter interface port *<port alias or number>* Displays IGMP Multicast Router information the specified interface. **Command mode:** All
show ip igmp mrouter portchannel *<trunk number>* Displays IGMP Multicast Router information the specified portchannel. **Command mode:** All
show ip igmp mrouter static Displays IGMP Multicast Router static 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 profile *<1-16>* Displays information about the current IGMP filter. **Command mode:** All
show ip igmp querier vlan *<VLAN number>* Displays IGMP Querier information. For details, see page 115. **Command mode:** All
show ip igmp snoop Displays IGMP Snooping information. **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 1.1.1.1,
 Switch-querier general query interval: 125 secs,
 Switch-querier max-response interval: 100 'tenths of secs',
 Switch-querier startup interval: 31 secs, count: 2
 Switch-querier robustness: 2
 IGMP configured version is v3
 IGMP Operating version is v3
```

IGMP Querier information includes:

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

IGMP Group Information

The following command displays IGMP Group information:

`show ip igmp groups`

Command mode: All

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

IGMP Group information includes:

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

IGMP Multicast Router Information

The following command displays Mrouter information:

`show ip igmp mrouter information`

Command mode: All

```
Total entries: 3
Total number of dynamic mrouters: 2
Total number of installed static mrouters: 1
SrcIP         VLAN    Port       Version   Expires   MRT       QRV   QQIC
------------- ------- -------    --------- --------  -------   ----  ----
10.1.1.1       3       EXT4       V3        4:09     128        2     125
10.1.1.5       2       EXT6       V2        4:09     125        -       -
*              9       EXT7       V2       static     -         -       -
```

IGMP Mrouter information includes:

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

IPMC Group Information

The following command displays IGMP IPMC group information:

`show ip igmp ipmcgrp`

Command mode: All

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

IGMP IPMC Group information includes:

- IGMPv3 source address
- Multicast group address
- VLAN and port
- Type of IPMC group
- Expiration timer value

MLD information

Table 54 describes the commands used to view Multicast Listener Discovery (MLD) information.

Table 54. *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
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 119 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 55. *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.
  - `holdoff` identifies that the virtual router is in holdoff state.
  - `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 fd55:faaf:e1ab:1022:7699:75ff:fe91:a6ef/64  , vlan 4095, up
            fe80::7699:75ff:fe91:a6ef
  128:    IP4 9.37.78.51      255.255.252.0   9.37.79.255 , 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 56. *IKEv2 Information Commands*

Command Syntax and Usage
show ikev2 Displays all IKEv2 information. See page 126 for sample output. **Command mode:** All
show ikev2 ca-cert Displays the CA certificate. **Command mode:** All
show ikev2 host-cert Displays the host certificate. **Command mode:** All
show ikev2 identity Displays IKEv2 identity information. **Command mode:** All
show ikev2 preshare-key Displays the IKEv2 preshare key. **Command mode:** All
show ikev2 proposal Displays the IKEv2 proposal. **Command mode:** All
show ikev2 retransmit-interval Displays the IKEv2 retransmit interval. **Command mode:** All
show ikev2 sa Displays the IKEv2 SA. **Command mode:** All

IKEv2 Information Dump

The following command displays IKEv2 information:

`show ikev2`

Command mode: All

```
IKEv2 retransmit time:       20

IKEv2 cookie notification:   disable

IKEv2 authentication method: Pre-shared key

IKEv2 proposal:
Cipher:                      3des
Authentication:              sha1
DH Group:                    dh-2

Local preshare key:          lenovo123

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 57. *IPsec Information Commands*

Command Syntax and Usage
show ipsec dynamic-policy *<1-10>* Displays dynamic policy information. **Command mode:** All
show ipsec manual-policy *<1-10>* Displays manual policy information. See page 128 for sample output. **Command mode:** All
show ipsec sa Displays all security association information. **Command mode:** All
show ipsec spd Displays all security policy information. **Command mode:** All
show ipsec traffic-selector *<1-10>* Displays IPsec traffic selector information. **Command mode:** All
show ipsec transform-set *<1-10>* Displays IPsec transform set information. **Command mode:** All

IPsec Manual Policy Information

The following command displays IPsec manual key management policy information:

`show ipsec manual-policy`

Command mode: All

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

IPsec manual policy information includes:

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

PIM Information

The following commands display PIM information.

Table 58. *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 130. **Command mode:** All
show ip pim elected-rp [group <*multicast group address*>**]** Displays a list of the elected Rendezvous Points. **Command mode:** All
show ip pim interface [<*interface number*>**|detail|port** <*port number*>**]** Displays PIM interface information. To view sample output, see page 130. **Command mode:** All
show ip pim mroute [<*component ID*>**|count|flags|** **|group** <*multicast group address*>**|interface {**<*interface number*>**|** **|port** <*port number*>**}|source** <*multicast source address*>**]** Displays information about PIM multicast routes. For more information about displaying PIM multicast route information, see page 132. **Command mode:** All
show ip pim neighbor [<*interface number*>**|port** <*port number*>**]** Displays PIM neighbor information. To view sample output, see page 131. **Command mode:** All
show ip pim neighbor-filters Displays information about PIM neighbor filters. **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

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: 1.1.1.1
  Candidate RP Holdtime: 100
```

```
PIM Component Information
--------------------------
Component-Id: 1
  PIM Mode: dense,   PIM Version: 2
  Graft Retry Count: 1
```

PIM component information includes the following:

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

PIM Interface Information

The following command displays information about PIM interfaces:

`show ip pim interface`

Command mode: All

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

PIM interface information includes the following for each PIM interface:

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

PIM Neighbor Information

The following command displays PIM neighbor information:

`show ip pim neighbor`

Command mode: All

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

PIM neighbor information includes the following:

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

PIM Multicast Route Information Commands

The following commands display PIM Multicast Route information.

Table 59. *PIM Multicast Route Information Options*

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

PIM Multicast Route Information

The following command displays PIM multicast route information:

`show ip pim mroute`

Command mode: All

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

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

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

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

Quality of Service Information

The following commands display Quality of Service information.

Table 60. *QoS Information Options*

Command Syntax and Usage
show qos dscp Displays the current DSCP parameters. **Command mode:** All
show qos protocol-packet-control information protocol Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. **Command mode:** All
show qos protocol-packet-control information queue [all] 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 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. For details, see page 135. **Command mode:** All
show qos random-detect Displays WRED ECN information. **Command mode:** All

802.1p Information

The following command displays 802.1p information:

`show qos transmit-queue information`

Command mode: All

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

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
INT1        0       0      1
INT2        0       0      1
...
MGT1        0       0      1
MGT2        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 61. *802.1p Priority-to-COS Queue Parameter Descriptions*

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

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

Table 62. *802.1p Port Priority Parameter Descriptions*

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

WRED and ECN Information

The following command displays WRED and ECN information:

`show qos random-detect`

Command mode: All

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

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

Access Control List Information Commands

The following commands display Access Control List information.

Table 63. *ACL Information Options*

Command Syntax and Usage
show access-control group [*<1-256>***]** Displays ACL group information. **Command mode:** All
show access-control list [*<1-256>***]** Displays ACL list information. For details, see page 138. **Command mode:** All
show access-control list6 [*<1-128>***]** Displays IPv6 ACL list information. **Command mode:** All
show access-control vmap [*<1-128>***]** Displays VMAP information. **Command mode:** All

Access Control List Information

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

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

Command mode: All

```
Current ACL information:
------------------------
  Filter 2 profile:
   Ethernet
     - VID        : 2/0xfff
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Actions        : Permit
   Statistics     : enabled
```

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

Table 64. *ACL Parameter Descriptions*

Parameter	Description
Filter *x* profile	Indicates the ACL number.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
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 65. *RMON Information commands*

Command Syntax and Usage
show rmon Displays all RMON information. **Command mode:** All
show rmon alarm [*<alarm group number>***]** Displays RMON Alarm information. For details, see page 141. **Command mode:** All
show rmon event [*<event group number>***]** Displays RMON Event information. For details, see page 142. **Command mode:** All
show rmon history [*<history group number>***]** Displays RMON History information. For details, see page 140. **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 66. *RMON History Parameter Descriptions*

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

RMON Alarm Information

The following command displays RMON Alarm information:

`show rmon alarm`

Command mode: All

```
RMON Alarm group configuration:

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

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

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

The following table describes the RMON Alarm Information parameters.

Table 67. *RMON Alarm Parameter Descriptions*

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

Table 67. *RMON Alarm Parameter Descriptions (continued)*

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

RMON Event Information

The following command displays RMON 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 68. *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
```

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 Lenovo Switch 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 Information

The following command displays port information:

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

Command mode: All

```
Alias   Port Tag   Type     RMON Lrn Fld PVID   DESCRIPTION  VLAN(s)
             Trk                        NVLAN
------- ---- --- --------- ---- --- --- ------ ----------- --------
INTA1   1     n  Internal    d    e   e  4081#  INTA1          4081
INTA2   2     n  Internal    d    e   e  4081#  INTA2          4081
INTA3   3     n  Internal    d    e   e  4081#  INTA3          4081
INTA4   4     n  Internal    d    e   e  4081#  INTA4          4081
INTA5   5     n  Internal    d    e   e  4081#  INTA5          4081
INTA6   6     n  Internal    d    e   e  4081#  INTA6          4081
INTA7   7     n  Internal    d    e   e  4081#  INTA7          4081
INTA8   8     n  Internal    d    e   e  4081#  INTA8          4081
INTA9   9     n  Internal    d    e   e  4081#  INTA9          4081
INTA10  10    n  Internal    d    e   e  4081#  INTA10         4081
INTA11  11    n  Internal    d    e   e  4081#  INTA11         4081
INTA12  12    n  Internal    d    e   e  4081#  INTA12         4081
INTA13  13    n  Internal    d    e   e  4081#  INTA13         4081
INTA14  14    n  Internal    d    e   e  4081#  INTA14         4081
INTB1   15    n  Internal    d    e   e  4082#  INTB1          4082
INTB2   16    n  Internal    d    e   e  4082#  INTB2          4082
INTB3   17    n  Internal    d    e   e  4082#  INTB3          4082
INTB4   18    n  Internal    d    e   e  4082#  INTB4          4082
INTB5   19    n  Internal    d    e   e  4082#  INTB5          4082
INTB6   20    n  Internal    d    e   e  4082#  INTB6          4082
INTB7   21    n  Internal    d    e   e  4082#  INTB7          4082
INTB8   22    n  Internal    d    e   e  4082#  INTB8          4082
INTB9   23    n  Internal    d    e   e  4082#  INTB9          4082
INTB10  24    n  Internal    d    e   e  4082#  INTB10         4082
INTB11  25    n  Internal    d    e   e  4082#  INTB11         4082
INTB12  26    n  Internal    d    e   e  4082#  INTB12         4082
INTB13  27    n  Internal    d    e   e  4082#  INTB13         4082
INTB14  28    n  Internal    d    e   e  4082#  INTB14         4082
INTC1   29    n  Internal    d    e   e  4083#  INTC1          4083
INTC2   30    n  Internal    d    e   e  4083#  INTC2          4083
INTC3   31    n  Internal    d    e   e  4083#  INTC3          4083
INTC4   32    n  Internal    d    e   e  4083#  INTC4          4083
INTC5   33    n  Internal    d    e   e  4083#  INTC5          4083
INTC6   34    n  Internal    d    e   e  4083#  INTC6          4083
...
EXT21   63    n  External    d    e   e     1   EXT21          1
EXT22   64    n  External    d    e   e     1   EXT22          1
EXTM    65    n  Mgmt        d    e   e  4095   EXTM           4095
MGT1    66    y  Mgmt        d    e   e  4095   MGT1           4095

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

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 Lenovo Switch 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`)
- Whether the port uses PVID/Native-VLAN tagging or not (`y` or `n`)
- Whether the port uses PVID ingress tagging or not (`y` or `n`)
- Whether the port is internal, external or used for 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/Native-VLAN)
- Port description
- 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

```
Port           Link  Transceiver    Vendor           Part        Approve
-------------- ----- ----------- -------------- -------------- ---------
EXT1 SFP+  1     < NO Device Installed >
EXT2 SFP+  2   Down  CU SFP      IBM-Finisar     78P3177-N81713  Approved
EXT3 Q10G 3.1    < NO Device Installed >
EXT4 Q10G 3.2    < NO Device Installed >
EXT5 Q10G 3.3    < NO Device Installed >
EXT6 Q10G 3.4    < NO Device Installed >
EXT7 Q10G 4.1    < NO Device Installed >
EXT8 Q10G 4.2    < NO Device Installed >
EXT9 Q10G 4.3    < NO Device Installed >
EXT10 Q10G 4.4   < NO Device Installed >
EXT11 FLEX  1    < NO Device Installed >
EXT12 FLEX  2    < NO Device Installed >
EXT13 FLEX  3  Down  3m ACTX     IBM-Amphenol    46K6183-L36836B Accepted
EXT14 FLEX  4    < NO Device Installed >
EXT15 FLEX  5    < NO Device Installed >
EXT16 FLEX  6    < NO Device Installed >
EXT17 FLEX  7    < NO Device Installed >
EXT18 FLEX  8  LINK  3m DAC      BLADE NETWORKS  BN-SP-CBL-3M    Accepted
EXT19 FLEX  9    < NO Device Installed >
EXT20 FLEX 10  LINK  1m DAC      BLADE NETWORKS  BN-SP-CBL-1M    Accepted
EXT21 FLEX 11    < NO Device Installed >
EXT22 FLEX 12    < NO Device Installed >
```

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

- Port number and media type
- Link status
- Transceiver detail
- Vendor information
- Part number
- Approval state

Use the following command to display extended transceiver information:

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

Command mode: All

```
Port       TX  Link  TXFlt Volts DegsC TXuW  RXuW  Transceiver Approve
---------- --- ----- ----- ----- ----- ----- ----- ----------- --------
55 FLEX  3 Ena Down  -N/A- -N/A- -N/A- -N/A- -N/A- 3m ACTX     Accepted
    IBM-Amphenol  Part:46K6183-L36836B  Date:111231 S/N:YL11FY1CY40G
```

This command displays detailed information about the transceiver module, as follows:

- Port number and media type
- TX: Transmission status
- 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)
- 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 69. *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.

VM Ready Information

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

Table 70. *Virtual Machines Information Options*

Command Syntax and Usage
show virt oui Displays all the configured MAC OUIs. **Command mode:** All
show virt port *<port alias or number>* Displays VM Ready information for the selected port. **Command mode:** All
show virt portchannel *<portchannel group member>* Displays Virtual Machine information for the selected portchannel. **Command mode:** All
show virt vm [-v|-r] Displays all VM Ready information. o `-v` displays verbose information o `-r` rescans the data center **Command mode:** All
show virt vmcheck Displays the current VM Check settings. **Command mode:** All
show virt vmgroup [*<1-4096>***]** Displays the current VM Group parameters. **Command mode:** All
show virt vmpolicy vmbandwidth **[***<MAC address>***|***<UUID>***|***<name>***|***<IP address>***|***<index number>***]** Displays the current VM bandwidth management parameters. **Command mode:** All
show virt vmprofile [*<profile name>***]** Displays the current VM Profile parameters. **Command mode:** All
show virt vmware Displays the current VMware parameters. **Command mode:** All

VM Information

The following command displays VM Ready information:

`show virt vm`

Command mode: All

```
IP Address       VMAC Address      Index Port    VM Group (Profile) Check Status
---------------- ----------------- ----- ------- ------------------ ------------
*127.31.46.50    00:50:56:4e:62:f5 4     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: 7
* indicates VMware ESX Service Console Interface
+ indicates VMware ESX/ESXi VMKernel or Management Interface
```

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

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

VM Check Information

The following command displays VM Check information:

`show virt vmcheck`

Command mode: All

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

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

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 71. *VMware Information Options*

Command Syntax and Usage
show virt vmware hosts Displays a list of VMware hosts. **Command mode:** All
show virt vmware hello Displays VMware hello settings. **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 switchport-mapping Displays ESX Server - switchport mapping. **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.

EVB Information

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

Table 72. *EVB Information Options*

Command Syntax and Usage
show virt evb profile [ports] Displays all EVB profile parameters. The `ports` option also display port parameters. **Command mode:** All
show virt evb profile *<1-16>* **[ports]** Displays the selected EVB profile parameters. The `ports` option also display port parameters. **Command mode:** All
show virt evb vdp vm Displays all active Virtual Machines (VMs). **Command mode:** All
show virt evb vdp tlv Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs). **Command mode:** All
show virt evb vsidb *<VSI_database_number>* Displays Virtual Station Interface database information. **Command mode:** All
show virt evb vsitypes [mgrid *<0-255>***|typeid** *<1-16777215>***| |version** *<0-255>***]** Displays the current Virtual Station Interface Type database parameters. **Command mode:** All

vNIC Information

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

Table 73. *vNIC Information Options*

Command Syntax and Usage
show vnic information-dump Displays all vNIC information. **Command mode:** All
show vnic vnic Displays information about each vNIC. **Command mode:** All
show vnic vnicgroup Displays information about each vNIC Group, including: o Status (enabled or disabled) o VLAN assigned to the vNIC Group o Uplink Failover status (enabled or disabled) o Link status for each vNIC (up, down, or disabled) o Port link status for each port associated with the vNIC Group (up, down, or disabled) **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
-------  ---------  -----  ------------  ------- ------------------ ----
INT1.1   1          100    25            Default  00:00:c9:c6:d0:2a   up
INT1.2   #          *      0             FCoE     00:00:c9:c6:d0:2b   up
INT1.3   3          300    25            Default  00:00:c9:c6:d0:2c   up
INT1.4   4          400    25            Default  00:00:c9:c6:d0:2d   up
INT2.1   1          100    25            Default  00:00:c9:c6:cf:72   up
INT2.2   #          *      0             FCoE     00:00:c9:c6:cf:73   up
INT2.3   3          300    25            Default  00:00:c9:c6:cf:74   up
INT2.4   4          400    25            Default  00:00:c9:c6:cf:75   up
INT3.1   1          100    25            Default  00:00:c9:e3:09:5c   up
INT3.3   3          300    25            Default  00:00:c9:e3:09:5e   up
INT3.4   4          400    25            Default  00:00:c9:e3:09:5f   up
INT4.2   #          *      0             FCoE     00:00:c9:b2:55:6f   up
INT9.2   #          *      0             FCoE     00:00:c9:c6:cf:33   up
# = 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         : 100
Failover     : disabled

vNIC        Link
----------  ---------
INT1.1      up
INT2.1      up
INT3.1      up

Port        Link
----------  ---------

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 74. *SLP Information Options*

Command Syntax and Usage
show ip slp directory-agents Lists all detected Directory Agents (DAs). **Command mode**: All
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 user-agents Lists all detected User Agents (UAs). **Command mode**: All

UFP Information

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

Table 75. *UFP Information Options*

Command Syntax and Usage
show ufp [port *<port_no.>***] [vport** *<1-4>***] [network|qos|evb]** Displays the UFP network and QoS settings applied on all ports or on specified physical and virtual ports. o `network` filters only UFP network settings o `qos` filters only QoS network settings o `evb` filters only EVB profile settings **Command mode:** All
show ufp information {cdcp|qos|tlvstat} [port *<port_no.>***]** Displays global or port-specific UFP information on: o `cdcp` displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see page 158. o `qos` displays bandwidth allocation between virtual ports. For details, see page 158. o `tlvstat` displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see page 159. **Command mode:** All
show ufp information getvlan *<2-4094>* Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID. **Command mode:** All
show ufp information port [*<port_no.>***]** Displays UFP status for all physical ports or only for a specified physical port. Information includes wether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see page 157. **Command mode:** All
show ufp information qos [port *<port_no.>***] [vport** *<1-4>***]** Displays bandwidth allocation between virtual ports for all physical ports or specified physical and virtual ports. For details, see page 158. **Command mode:** All

Table 75. *UFP Information Options*

Command Syntax and Usage
show ufp information vport [port *<port_no.>***] [vport** *<1-4>***]** Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see page 160. **Command mode:** All
show ufp information vlan [*<1-4094>***]** Displays ports and vports associated to all configured VLANs or to a specified VLAN ID. For details, see page 161. **Command mode:** All

Port Information

The following command displays UFP port information:

show ufp information port

Command mode: All

```
Alias   Port   state   vPorts   link up   link down   mismatch   disabled
-----   ----   -----   ------   -------   ---------   --------   --------
INTA4    4     ena        4     1  3  4                  2
```

Port information includes the following for each physical port:

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

CDCP Information

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

`show ufp information cdcp`

Command mode: All

```
INT1  : Channel Request
INT2  : Channel Request
INT3  :         TxSVIDs
INT4  :         TxSVIDs
INT5  :         Disable
INT6  :         Disable
INT7  :         Disable
INT8  :         Disable
INT9  :         Disable
INT10 :         Disable
INT11 :         Disable
INT12 :         Disable
INT13 :         Disable
INT14 :         Disable
```

CDCP information includes the following for each physical port:

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

QoS Information

The following command displays Quality of Service information:

`show ufp information qos`

Command mode: All

```
Global UFP QOS mode: UFP QOS BW

Port | Vport | Minbw%| Maxbw%
------------------------------
1    | 1     | 15    | 100
     | 2     | 25    |  50
     | 3     | 25    | 100
     | 4     | 25    | 100
------------------------------
2    | 1     | 25    | 100
     | 2     | 25    | 100
     | 3     | 25    | 100
     | 4     | 25    | 100
------------------------------
3    | 1     | 25    | 100
     | 2     | 25    | 100
     | 3     | 25    | 100
     | 4     | 25    | 100
...
```

QoS information includes the following:

- Physical port number
- Virtual port number
- Minimum guaranteed bandwidth allocated
- Maximum bandwidth achievable

TLV Status Information

The following command displays Type-Length-Values information:

`show ufp information tlvstat`

Command mode: All

```
INT1  :         Success
INT2  :         Success
INT3  :        Disabled
INT4  :        Disabled
INT5  :        Disabled
INT6  :        Disabled
INT7  :        Disabled
INT8  :        Disabled
INT9  :        Disabled
INT10 :        Disabled
INT11 :        Disabled
INT12 :        Disabled
INT13 :        Disabled
INT14 :        Disabled
```

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

Virtual Port Information

The following command displays virtual port information:

`show ufp information vport`

Command mode: All

```
vPort      state   mode   svid  defvlan  deftag  evbprof  VLANs
---------  -----  ------  ----  -------  ------  -------  ---------------
 INTA1.1    dis   tunnel  0     0        dis       dis
 INTA1.2    dis   tunnel  0     0        dis       dis
 INTA1.3    dis   tunnel  0     0        dis       dis
 INTA1.4    dis   tunnel  0     0        dis       dis
 …
 INTA14.4   dis   tunnel  0     0        dis       dis
 INTB1.1    dis*  access  4002  100      dis       dis    100
 INTB1.2    up    fcoe    2500  2500     dis       dis    2500
 INTB1.3    dis*  trunk   4004  300      dis       dis    300 500
 INTB1.4    dis   tunnel  0     0        dis       dis
 INTB2.1    dis*  access  4002  100      dis       dis    100
 INTB2.2    up    fcoe    2500  2500     dis       dis    2500
 INTB2.3    dis*  trunk   4004  300      dis       dis    300 500
 INTB2.4    dis   tunnel  0     0        dis       dis
 INTB3.1    dis*  access  4002  100      dis       dis    100
 INTB3.2    up    fcoe    2500  2500     dis       dis    2500
 INTB3.3    dis*  trunk   4004  300      dis       dis    300 500
 INTB3.4    dis   tunnel  0     0        dis       dis
```

Virtual port information includes the following for each virtual port:

- Virtual port number
- Channel status
- Operating mode (trunk, access, tunnel, auto or FCoE)
- S-channel VLAN ID
- Default VLAN ID
- Default VLAN ID tagging enforcement
- EVB profile
- VLANs the virtual port is associated with

VLAN Information

The following command displays VLAN information:

`show ufp information vlan`

Command mode: All

```
VLAN
----
 100

vPort list:
  INTB1.1    INTB2.1    INTB3.1    INTB4.1    INTB5.1    INTB6.1
  INTB7.1    INTB8.1    INTB9.1    INTB10.1   INTB11.1   INTB12.1

EXT Port list:
  EXT3     EXT4     EXT8     EXT9

INT Port list:
  INTB13

UFP Port list:
  INTB1    INTB2    INTB3    INTB4    INTB5    INTB6    INTB7    INTB8
  INTB9   INTB10    INTB11   INTB12

VMR Port list:
```

VLAN information includes the following for each VLAN:

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

TLV Information

The following commands display TLV information:

`show ufp {receive|transmit} cap port` *<port_no.>*

Command mode: All

```
UFP Capability Discovery TLV Received on port INT2:
    tlv     : Type 127 Length 7 OUI 00-18-b1 Subtype 1
    version : Max 1 Oper 1
    cna     : Req 1 Oper 1 Res 0x00
    switch  : Cap 1 Oper 1 Res 0x00
```

UFP Capability Discovery TLV information includes the following:

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

`show ufp {receive|transmit} cdcp port` *<port_no.>*

Command mode: All

```
CDCP TLV Transmitted on port INT2:
    tlv     : Type 127 Length 23 OUI 00-80-c2 Subtype 14
    local   : Role 0 SComp 1 Channel Cap 5
    SCID 1  : SVID 1
    SCID 2  : SVID 4002
    SCID 3  : SVID 4003
    SCID 4  : SVID 0
    SCID 5  : SVID 0
```

UFP Channel Discovery and Configuration Protocol TLV includes the following:

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

DCBX Information Commands

The following commands display DCBX information.

Table 76. *DCBX Information Commands*

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

Converged Enhanced Ethernet Information

Table 77 describes the Converged Enhanced Ethernet (CEE) information options.

Table 77. *CEE Information Options*

Command Syntax and Usage
show cee global {ets|pfc} [information] Displays global ETS or PFC information. **Command mode:** All
show cee [information] Displays all CEE information. **Command mode:** All
show cee iscsi Displays the current ISCSI TLV parameters. **Command mode**: All
show cee port *<port alias or number>* Displays CEE information for the specified port. **Command mode:** All

DCBX Information

Table 78 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 78. *DCBX Information Options*

Command Syntax and Usage
show cee information dcbx port *<port alias or number>* Displays all DCBX information. **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 170. **Command mode:** All
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 166. **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 168. **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 167. **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 169. **Command mode:** All

DCBX Control Information

The following command displays DCBX control information:

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

Command mode: All

```
DCBX Port Control State-machine Info
================================================
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
------ ---- ------- -------- ---- ----- ----- ----- ------ ----- --- -------- -----
INTA2  2    ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA2  2    PFC     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA2  2    AppProt disabled No   Yes   0     0     Yes    1     No  disabled Yes
...
```

The following table describes the DCBX feature information.

Table 79. *DCBX Feature Information Fields*

Parameter	Description
Alias	Displays each port's alias.
Port	Displays each port's number.
Type	Feature type.
AdmState	Feature status (Enabled or Disabled).
Will	Willing flag status (Yes/True or No/Untrue).
Advrt	Advertisement flag status (Yes/True or No/Untrue).
OpVer	Operating version negotiated with the peer device.
MxVer	Maximum operating version supported by the system.
PrWill	Peer's Willing flag status (Yes/True or No/Untrue).
SeqNo	Sequence number that changes each time a DCBX parameter in one or more DCB feature TLVs changes.
Err	Error condition flag (Yes or No). Yes indicates that an error occurred during the exchange 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   PGID1    PGID1
INTA2  2    4        PGID2   PGID2    PGID0
INTA2  2    5        PGID2   PGID2    PGID0
INTA2  2    6        PGID2   PGID2    PGID0
INTA2  2    7        PGID2   PGID2    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 80. *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.
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
------ ---- -------- ---------- ---------- ----------
INTA2  2    0        disabled   disabled   disabled
INTA2  2    1        disabled   disabled   disabled
INTA2  2    2        disabled   disabled   disabled
INTA2  2    3        enabled    enabled    enabled
INTA2  2    4        disabled   disabled   disabled
INTA2  2    5        disabled   disabled   disabled
INTA2  2    6        disabled   disabled   disabled
INTA2  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
------ ---- -------- ---------- ---------- ----------
INTA2  2    0        disabled   disabled   disabled
INTA2  2    1        disabled   disabled   disabled
INTA2  2    2        disabled   disabled   disabled
INTA2  2    3        enabled    disabled   enabled
INTA2  2    4        disabled   disabled   disabled
INTA2  2    5        disabled   disabled   disabled
INTA2  2    6        disabled   disabled   disabled
INTA2  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
------ ---- -------- ---------- ---------- ----------
INTA2  2    0        disabled   disabled   disabled
INTA2  2    1        disabled   disabled   disabled
INTA2  2    2        disabled   disabled   disabled
INTA2  2    3        enabled    disabled   disabled
INTA2  2    4        disabled   disabled   disabled
INTA2  2    5        disabled   disabled   disabled
INTA2  2    6        disabled   disabled   disabled
INTA2  2    7        disabled   disabled   disabled
```

The following table describes the DCBX Application Protocol information.

Table 81. *DCBX Application Protocol Information Fields*

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: o 0 = Ethernet Type o 1 = TCP socket ID
Organizationally Unique ID	DCBX TLV identifier

Table 81. *DCBX Application Protocol Information Fields (continued)*

Parameter	Description
Alias	Port alias
Port	Port number
Priority	802.1p value
EnableDesr	Status configured on this switch
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

ETS Information

Table 82 describes the Enhanced Transmission Selection (ETS) information options.

Table 82. *ETS Information Options*

Command Syntax and Usage
show cee global ets [information] Displays global ETS information. **Command mode:** All
show cee global ets priority-group *<0-7, 15>* Displays the current global ETS Priority Group parameters. **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 83 describes the Priority Flow Control (PFC) information options.

Table 83. *PFC Information Options*

Command Syntax and Usage
show cee global pfc [information] Displays global PFC information. **Command mode:** All
show cee global pfc priority *<priority value>* Displays the current global PFC 802.1p priority parameters. **Command mode:** All
show cee port *<port alias or number>* **pfc [information]** Displays PFC information on the specified port. **Command mode:** All
show cee port *<port alias or number>* **pfc priority** *<priority value>* Displays the current PFC 802.1p priority parameters for the specified port. **Command mode:** All

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

Table 84. *FCoE Information Options*

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

FIP Snooping Information

Table 85 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options.

Table 85. *FIP Snooping Information Options*

Command Syntax and Usage
`show fcoe fips [information]` Displays FIP Snooping information for all ports. **Command mode:** All
`show fcoe fips fcf` Displays FCF information for all FCFs learned. **Command mode:** All
`show fcoe fips fcoe` Displays FCoE connections established on the switch. **Command mode:** All
`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 vlans` Displays VLAN information. **Command mode:** All

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

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

Command mode: All

```
FIP Snooping on port INTA2:
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:

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

Fibre Channel Information

These commands allow you to display Fibre Channel information.

Table 86. *Fibre Channel Information Commands*

Command Syntax and Usage
show flogi database [<*switch_number*>**]** Displays fabric login database information. For details, see page 178. **Command mode:** All
show fcalias [<*switch_number*>**]** Displays the current FC alias - PWWN (port World Wide Name) mapping. **Command mode:** All
show fcdomain [<*switch_number*>**]** Displays the current configuration of FC domains. **Command mode:** All
show fcns database [<*switch_number*>**]** Displays FC name server database information. For details, see page 178. **Command mode:** All
show fdmi database [<*switch_number*>**]** Displays fibre channel management interface database information. **Command mode:** All
show fcs database [<*switch_number*>**]** Displays fabric configuration status database information. For details, see page 179. **Command mode:** All
show fcoe database [<*switch_number*>**]** Displays Fibre Channel over Ethernet database information. **Command mode:** All
show fcf [<*switch_number*>**]** Displays Fibre Channel forwarding information. For details, see page 179. **Command mode:** All
show npv status [<*switch_number*>**]** Displays N_Port Virtualization information. **Command mode:** All
show npv flogi-table [<*switch_number*>**]** Displays the contents of the NPV fabric login table. **Command mode:** All

Table 86. *Fibre Channel Information Commands*

Command Syntax and Usage
show npv traffic-map [<*switch_number*>**]** Displays NPV source-destination traffic mapping. For details, see page 180. **Command mode:** All
show zone [<*switch_number*>**]** Lists all FC zones. **Command mode:** All
show zone status [<*switch_number*>**]** Displays FC zone status information. For details, see page 180. **Command mode:** All
show zone name <*zone name*> **[**<*switch_number*>**]** Displays information for the specified FC zone. **Command mode:** All
show zoneset [<*switch_number*>**]** Lists all FC zonesets. **Command mode:** All
show zoneset name <*zoneset name*> **[**<*switch_number*>**]** Displays information for the specified FC zoneset. **Command mode:** All
show zoneset active [<*switch_number*>**]** Displays the currently active FC zoneset. **Command mode:** All
show interface fc information [<*switch_number*>**]** Displays FC port information. For details, see page 181. **Command mode:** All
show interface fc port <*port no.*> **[**<*switch_number*>**]** Displays FC information for the specified ports. **Command mode:** All
show topology [<*switch_number*>**]** Displays port and corresponding node information for each switch member of the fabric or only for a specific switch member. For details, see page 182. **Command mode:** All
show steering [<*switch_number*>**]** Displays frame steering information for each switch member of the fabric or only for a specific switch member. **Command mode:** All

Table 86. *Fibre Channel Information Commands*

Command Syntax and Usage
show fabric Display the FC fabric information. **Command mode**: All
show lsdb Display the link state db information of the FC fabric. **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-map`

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 87. *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: o E (Expansion port) **not supported o F (Fabric port) o Eth (Ethernet port)
Running Type	Current operational FC port type, as follows: o E (Expansion port) **not supported o F (Fabric port) o Eth (Ethernet port) o 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
```

Topology Information

The following command displays a list of the ports and corresponding nodes for each switch member of the fabric:

`show topology`

Command mode: All

```
Information for Switch Unit 1:
(This is the local swunit)
Switch Domain Id   : 1
Switch Mgmt Id     : 010000
Fabric Name        : 10:00:6c:ae:8b:d6:11:c1
Switch WWN         : 10:00:6c:ae:8b:d6:11:c1
Switch Ports Online:
-----------------------------------------------------------------
Port        LocalPortWWN               RemoteNodeWWN
-----------------------------------------------------------------
EXT1        20:00:00:11:0d:64:f5:00    20:00:00:11:0d:64:f5:00
EXT2        20:01:00:11:0d:64:f4:00    20:01:00:11:0d:64:f4:00
```

Information Dump

The following command dumps switch information:

`show information-dump`

Command mode: All

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

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

Chapter 3. Statistics Commands

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

Table 88. *Statistics Commands*

Command Syntax and Usage
show counters Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see page 280. **Command mode:** All
show layer3 counters Displays Layer 3 statistics. **Command mode:** All
show ntp counters Displays Network Time Protocol (NTP) Statistics. See page 277 for a sample output and a description of NTP Statistics. **Command mode:** All
show snmp-server counters Displays SNMP statistics. See page 273 for sample output. **Command mode:** All

Forwarding Database Statistics

The following commands display Forwarding Database statistics.

Table 89. *Forwarding Database statistics commands*

Command Syntax and Usage
show mac-address-table counters [all] Displays Forwarding Database (FDB) statistics. The `all` options displays all FDB statistics (unicast and multicast). **Command mode:** All
show mac-address-table counters interface port *<port alias or number>* Displays Forwarding Database (FDB) statistics for the specified port. **Command mode:** All
show mac-address-table counters portchannel *<trunk group number>* Displays Forwarding Database (FDB) statistics for the specified trunk group. **Command mode:** All
show mac-address-table counters state {forward|trunk|unknown} Displays Forwarding Database (FDB) statistics by state: o `forward` displays FDB statistics for forwarding state MAC address entries o `trunk` displays FDB statistics for trunk state MAC address entries o `unknown` displays FDB statistics for unknown state MAC address entries **Command mode:** All
show mac-address-table counters static Displays Forwarding Database (FDB) statistics for static MAC address entries. **Command mode:** All
show mac-address-table counters unicast Displays Forwarding Database (FDB) statistics for unicast MAC address entries. **Command mode:** All
show mac-address-table counters vlan *<VLAN number>* Displays Forwarding Database (FDB) statistics for the specified VLAN. **Command mode:** All
clear mac-address-table counters Clears Forwarding Database (FDB) statistics. **Command mode:** All except User EXEC

Port Statistics

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

Table 90. *Port Statistics Commands*

Command Syntax and Usage
show interface counters Displays interface statistics. **Command mode:** All
show interface port *<port alias or number>* **all-counters** Displays all statistics for the specified port. **Command mode:** All
show interface port *<port alias or number>* **bridging-counters** Displays bridging ("dot1") statistics for the specified port. See page 193 for sample output. **Command mode:** All
show interface port *<port alias or number>* **dot1x counters** Displays IEEE 802.1X statistics for the specified port. See page 189 for sample output. **Command mode:** All
show interface port *<port alias or number>* **ethernet-counters** Displays Ethernet ("dot3") statistics for the specified port. See page 194 for sample output. **Command mode:** All
show interface port *<port alias or number>* **interface-counters** Displays interface statistics for the specified port. See page 197 for sample output. **Command mode:** All
show interface port *<port alias or number>* **ip-counters** Displays IP statistics for the specified port. See page 200 for sample output. **Command mode:** All
show interface port *<port alias or number>* **link-counters** Displays link statistics for the specified port. See page 200 for sample output. **Command mode:** All
show interface port *<port alias or number>* **link-counters oam counters** Displays OAM link statistics for the specified port. **Command mode:** All

Table 90. *Port Statistics Commands*

Command Syntax and Usage
`show interface port` *<port alias or number>* **`maintenance-counters`** Displays maintenance statistics for the specified port. **Command mode:** All
`show interface port` *<port alias or number>* **`oam counters`** Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port. **Command mode:** All
`show interface port` *<port alias or number>* **`rmon-counters`** Displays Remote Monitoring (RMON) statistics for the port. See page 201 for sample output. **Command mode:** All
`clear counters` Clears statistics for all ports. **Command mode:** All except User EXEC
`clear interface port` *<port alias or number>* **`counters`** Clears all statistics for the port. **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 91. *802.1X Authenticator Statistics of a Port*

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

802.1X Authenticator Diagnostics

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

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

Command mode: All

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

Table 92. *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.
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.

Table 92. *802.1X Authenticator Diagnostics of a Port (continued)*

Statistics	Description
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 92. *802.1X Authenticator Diagnostics of a Port (continued)*

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 INT1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 93. *Bridging Statistics of a Port*

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

Ethernet Statistics

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

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

Command mode: All

```
Ethernet statistics for port INT1:
dot3StatsAlignmentErrors:                   0
dot3StatsFCSErrors:                         0
dot3StatsSingleCollisionFrames:             0
dot3StatsMultipleCollisionFrames:           0
dot3StatsLateCollisions:                    0
dot3StatsExcessiveCollisions:               0
dot3StatsInternalMacTransmitErrors:        NA
dot3StatsFrameTooLongs:                     0
dot3StatsInternalMacReceiveErrors:          0
```

Table 94. *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.

Table 94. *Ethernet Statistics for Port (continued)*

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

Table 94. *Ethernet Statistics for Port (continued)*

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

Interface Statistics

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

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

Command mode: All

```
Interface statistics for port EXT1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                            0                648329
UcastPkts:                         0                     0
BroadcastPkts:                     0                   271
MulticastPkts:                     0                  7654
FlowCtrlPkts:                      0                     0
PriFlowCtrlPkts:                   0                     0
Discards:                          0                    11
Errors:                            0                     0


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:             11
```

Table 95. *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 95. *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).

Table 95. *Interface Statistics for Port (continued)*

Statistics	Description
Policy Discards	Dropped due to policy setting. For example, due to a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of the Memory Management Unit.
Cell Error Discards	
MMU Aging Discards	
Other Discards	Discarded packets not included in any category.
Empty Egress Portmap	Dropped due to an egress port bitmap of zero condition (no ports in the egress mask). This counter increments whenever the switching decision found that there was no port to send out.

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 INT1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 96. *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 INT1:
linkStateChange:            1
```

Table 97. *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 98. *RMON Statistics of a Port*

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

Table 98. *RMON Statistics of a Port (continued)*

Statistics	Description
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).
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).

Table 98. *RMON Statistics of a Port (continued)*

Statistics	Description
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 Statistics

The following commands display Quality of Service (QoS) Queue statistics.

Table 99. *QoS Queue Statistics*

Command Syntax and Usage
show interface port *<port alias or number>* **egress-queue-counters [***<0-7>***|drop]** Displays the total number of successfully transmitted or dropped packets and bytes for each QoS queue for the selected port. o **<0-7>** displays statistics only for the specified queue o **drop** displays statistics only for the dropped packets and bytes **Command mode:** All
show interface port *<port alias or number>* **egress-mcast-queue-counters [***<8-11>***|drop]** Displays the total number of successfully transmitted or dropped packets and bytes for each multicast QoS queue for the selected port. o **<8-11>** displays statistics only for the specified queue o **drop** displays statistics only for the dropped packets and bytes **Command mode:** All
show interface port *<port alias or number>* **egress-queue-rate [***<0-7>***|drop]** Displays the number of successfully transmitted or dropped packets and bytes per second for each QoS queue for the selected port. o **<0-7>** displays statistics only for the specified queue o **drop** displays statistics only for the dropped packets and bytes **Command mode:** All
show interface port *<port alias or number>* **egress-mcast-queue-rate [***<8-11>***|drop]** Displays the number of successfully transmitted or dropped packets and bytes per second for each multicast QoS queue for the selected port. o **<8-11>** displays statistics only for the specified queue o **drop** displays statistics only for the dropped packets and bytes **Command mode:** All

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 100. *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.

Table 100. *QoS Queue Rate-Based Statistics of a Port (continued)*

Statistics	Description
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.

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

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

Command mode: All

```
QoS Rate for port 1:1:
QoS Queue 0:
    Tx Packets:                             0
    Dropped Packets:                        0
    Tx Bytes:                               0
    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 101. *QoS Queue Rate-Based Statistics of a Port*

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

Trunk Group Statistics

The following commands display Trunk Group statistics.

Table 102. *Trunk Group Statistics Commands*

Command Syntax and Usage
show interface portchannel *<trunk group number>* **interface-counters** Displays interface statistics for the trunk group. For a sample output see page 208. **Command mode:** All
clear interface portchannel *<trunk group number>* **counters** Clears all the statistics on the specified trunk group. **Command mode:** All except User EXEC

Trunk Group Interface Statistics

The following command displays interface statistics for the specified trunk group.

show interface portchannel *<trunk group number>* **interface-counters**

Command mode: All

```
Interface statistics for trunk group 12:
                     ifHCIn Counters       ifHCOut Counters
Octets:                     6003620              27746863
UcastPkts:                        0                     0
BroadcastPkts:                    0                 33358
MulticastPkts:                42883                135420
FlowCtrlPkts:                     0                     0
PriFlowCtrlPkts:                  0                     0
Discards:                         0                     0
Errors:                           0                     0

Ingress Discard reasons for trunk group 12:
VLAN Discards:                    0
Empty Egress Portmap:             0
Filter Discards:                  0
Policy Discards:                  0
Non-Forwarding State:             0
IBP/CBP Discards:                 0
```

Layer 2 Statistics

The following commands display Layer 2 statistics.

Table 103. *Layer 2 Statistics Commands*

Command Syntax and Usage
`show fcoe counters` Displays Fibre Channel over Ethernet (FCoE) statistics. See page 272 for sample output. **Command mode:** All
`show interface port` *<port alias or number>* **`lacp counters`** Displays Link Aggregation Control Protocol (LACP) statistics for the specified port. See page 210 for sample output. **Command mode:** All
`show interface port` *<port alias or number>* **`lldp counters`** Displays LLDP statistics for the specified port. See page 212 for sample output. **Command mode:** All except User EXEC
`show hotlinks counters` Displays Hot Links statistics. See page 211 for sample output. **Command mode:** All except User EXEC
`show oam counters` Displays OAM statistics. See page 213 for sample output. **Command mode:** All except User EXEC
`clear fcoe counters` Clears all Fibre Channel over Ethernet (FCoE) statistics. **Command mode:** All
`clear interface port` *<port alias or number>* **`lacp counters`** Clears all Link Aggregation Control Protocol (LACP) statistics for the specified port. **Command mode:** All except User EXEC
`clear interface port` *<port alias or number>* **`lldp counters`** Clears all LLDP statistics for the port. **Command mode:** All except User EXEC
`clear hotlinks` Clears all Hot Links statistics. **Command mode:** All except User EXEC

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 104. *LACP Statistics*

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

Hotlinks Statistics

Use the following command to display Hot Links statistics:

`show hotlinks counters`

Command mode: All

```
Hot Links Trigger Stats:
------------------------------------------------------------------------
Trigger 1 statistics:
    Trigger Name: Trigger 1
    Master active:           0
    Backup active:           0
    FDB update:              0   failed: 0
```

The following table describes the Hotlinks statistics:

Table 105. *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 INT1 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 106. *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 INT1
----------------------------------------
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 107. *vLAG Statistics Options*

Command Syntax and Usage
show vlag isl-statistics Displays vLAG ISL statistics for the selected port. See page 214 for sample output.
show vlag statistics Displays all vLAG statistics. See page 214 for sample output.
clear vlag statistics Clears all vLAG statistics.

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 108. *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.
`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.
`IGMP Reports`	Total number of IGMP Reports forwarded over vLAG.
`IGMP Leaves`	Total number of IGMP Leave messages forwarded over vLAG.

Layer 3 Statistics

The following commands display Layer 3 statistics.

Table 109. *Layer 3 Statistics Commands*

Command Syntax and Usage
show ip arp counters Displays Address Resolution Protocol (ARP) statistics. See page 230 for sample output. **Command mode:** All
show ip counters Displays IP statistics. See page 220 for sample output. **Command mode:** All
show ip dns counters Displays Domain Name System (DNS) statistics. See page 231 for sample output. **Command mode:** All
show ip icmp counters Displays ICMP statistics. See page 232 for sample output. **Command mode:** All
show ip igmp counters Displays IGMP statistics. See page 237 for sample output. **Command mode:** All
show ip igmp vlan *<VLAN number>* **counter** Displays IGMP statistics for a specific VLAN. See page 237 for sample output. **Command mode:** All
show ip pim counters Displays PIM statistics for all configured PIM interfaces. See page 252 for sample output. **Command mode:** All
show ip pim interface *<interface number>* **counters** Displays PIM statistics for the selected interface. **Command mode:** All
show ip pim mroute count Displays statistics of various multicast entry types. **Command mode:** All

Table 109. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
show ip ospf counters Displays OSPF statistics. See page 243 for sample output. **Command mode:** All
show ip rip counters Displays Routing Information Protocol (RIP) statistics. See page 253 for sample output. **Command mode:** All
show ip route counters Displays route statistics. See page 228 for sample output. **Command mode:** All
show ip slp counter Displays Service Location Protocol (SLP) packet statistics. See page 279 for a sample output. **Command mode:** All
show ip tcp counters Displays TCP statistics. See page 234 for sample output. **Command mode:** All
show ip udp counters Displays UDP statistics. See page 236 for sample output. **Command mode:** All
show ip vrrp counters When virtual routers are configured, you can display the protocol statistics for VRRP. See page 251 for sample output. **Command mode:** All
show ipv6 counters Displays IPv6 statistics. See page 223 for sample output. **Command mode:** All
show ipv6 mld counters Displays Multicast Listener Discovery (MLD) statistics. Command mode: All
show ipv6 ospf counters Displays OSPFv3 statistics. See page 248 for sample output. **Command mode:** All

Table 109. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
clear ip counters Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. **Command mode:** All except User EXEC
clear ip arp counters Clears Address Resolution Protocol (ARP) statistics. **Command mode:** All except User EXEC
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 igmp [*<VLAN number>***] counters** Clears IGMP statistics for all VLANs or for a specific VLAN. **Command mode:** All
clear ip ospf counters Clears Open Shortest Path First (OSPF) statistics. **Command mode:** All except User EXEC
clear ip rip counters Clears Routing Information Protocol (RIP) statistics. **Command mode:** All except User EXEC
clear ip slp counters Clears Service Location Protocol (SLP) packet 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 vrrp counters Clears VRRP statistics. **Command mode:** All

Table 109. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
clear ipv6 counters Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 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

```
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 110. *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.
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.

Table 110. *IP Statistics (continued)*

Statistic	Description
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.
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.

Table 110. *IP Statistics (continued)*

Statistic	Description
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).

Use the following command to clear IPv4 statistics:

`clear ip counters`

Command mode: All except User EXEC

IPv6 Statistics

The following command displays IPv6 statistics:

`show ipv6 counters`

Command mode: All

```
IPv6 Statistics
***************
48016 Rcvd               0 HdrErrors          0 TooBigErrors
    0 AddrErrors         0 FwdDgrams          0 UnknownProtos
    0 Discards       48016 Delivers       48155 OutRequests
    0 OutDiscards        0 OutNoRoutes        0 ReasmReqds
    0 ReasmOKs           0 ReasmFails
    0 FragOKs            0 FragFails          0 FragCreates
    0 RcvdMCastPkt     146 SentMCastPkts      0 TruncatedPkts
    0 RcvdRedirects      0 SentRedirects
ICMP Statistics
***************
Received :
43353 ICMPPkts           1 ICMPErrPkt        91 DestUnreach       0 TimeExcds
    0 ParmProbs          0 PktTooBigMsg   39512 ICMPEchoReq       0 ICMPEchoReps
    0 RouterSols         0 RouterAdv       1828 NeighSols      1922 NeighAdv
    0 Redirects         91 AdminProhib        0 ICMPBadCode
Sent :
43269 ICMPMsgs           0 ICMPErrMsgs        0 DstUnReach        0 TimeExcds
    0 ParmProbs          0 PktTooBigs         0 EchoReq       39512 EchoReply
    6 RouterSols         0 RouterAdv       1924 NeighSols      1827 NeighborAdv
    0 RedirectMsgs       0 AdminProhibMsgs
UDP statistics
**************
Received :
4679 UDPDgrams           0 UDPNoPorts         0 UDPErrPkts
Sent :
91 UDPDgrams
```

Table 111 describes the IPv6 statistics.

Table 111. *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).

Table 111. *IPv6 Statistics (continued)*

Statistic	Description
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
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 112. *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.

Table 112. *ICMP Statistics (continued)*

Statistic	Description
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

Table 113 describes the UDP statistics.

Table 113. *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).

Use the following command to clear IPv6 statistics:

```
clear ipv6 counters
```

Command mode: All except User EXEC

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
```

Table 114. *Route Statistics*

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

IPv6 Route Statistics

The following command displays IPv6 route statistics:

`show ipv6 route counters`

Command mode: All

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

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

Table 115. *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 116. *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 117. *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 118. *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 118. *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:           2048
tcpActiveOpens:           0   tcpPassiveOpens:        16
tcpAttemptFails:          0   tcpEstabResets:          0
tcpInSegs:             2035   tcpOutSegs:           1748
tcpRetransSegs:          21   tcpInErrs:               0
tcpCurrEstab:             1   tcpCurrConn:             5
tcpOutRsts:               0
```

Table 119. *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 119. *TCP Statistics (continued)*

Statistic	Description
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP `checksums`).
tcpCurEstab	The total number of outstanding TCP sessions in the ESTABLISHED state.
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 120. *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 IGMP protocol packets for all VLANs:

`show ip igmp counters`

Command mode: All

```
IGMP vlan 2 statistics:
-------------------------------------------------------------------------
rxIgmpValidPkts:                0   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:               0   rxIgmpGrpSpecificQueries:         0
rxIgmpGroupSrcSpecificQueries:  0   rxIgmpDiscardPkts:                0
rxIgmpLeaves:                   0   rxIgmpReports:                    0
txIgmpReports:                  0   txIgmpGrpSpecificQueries:         0
txIgmpLeaves:                   0   rxIgmpV3CurrentStateRecords:      0
rxIgmpV3SourceListChangeRecords:0   rxIgmpV3FilterChangeRecords:      0
txIgmpGenQueries:               18  rxPimHellos:                      0
```

The following command displays statistics about IGMP protocol packets for a specific VLAN:

`show ip igmp vlan` *<VLAN number>* **`counter`**

Command mode: All

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

Table 121. *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 for specific groups.
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received.
rxIgmpDiscardPkts	Total number of IGMP packets discarded.

Table 121. *IGMP Statistics*

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

MLD Statistics

The following commands display MLD statistics.

Table 122. *MLD Statistics Commands*

Command Syntax and Usage
show ipv6 mld Displays MLD global statistics. See page 240 for sample output. **Command mode:** All
show ipv6 mld counters Displays MLD area statistics. **Command mode:** All
show ipv6 mld interface Displays information for all MLD interfaces. **Command mode:** All
show ipv6 mld interface counters Displays total number of MLD entries. **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 MLD interface statistics. **Command mode:** All
clear ipv6 mld counters Clears MLD counters. **Command mode:** Privileged EXEC
clear ipv6 mld dynamic Clears all dynamic MLD tables. **Command mode:** Privileged EXEC
clear ipv6 mld groups Clears dynamic MLD registered group tables. **Command mode:** Privileged EXEC
clear ipv6 mld mrouter Clears dynamic MLD mrouter group tables. **Command mode:** Privileged EXEC

MLD Global Statistics

The MLD global statistics displays information 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 123. *MLD Global Statistics*

Statistic	Description
Bad Length	Number of messages received with length errors.
Bad Checksum	Number of messages received with an invalid IP checksum.
Bad Receive If	Number of messages received on an interface not enabled for MLD.
Receive non-local	Number of messages received from non-local senders.
Invalid packets	Number of rejected packets.
General Query (v1/v2)	Number of general query packets.
MAS Query(v1/v2)	Number of multicast address specific query packets.
MASSQ Query (v2)	Number of multicast address and source specific query packets.
Listener Report(v1)	Number of packets sent by a multicast listener in response to MLDv1 query.
Listener Done(v1/v2)	Number of packets sent by a host when it wants to stop receiving multicast traffic.
Listener Report(v2)	Number of packets sent by a multicast listener in response to MLDv2 query.
MLDv2 INC mode CSRs	Number of current state records with include filter mode.
MLDv2 EXC mode CSRs	Number of current state records with exclude filter mode.
MLDv2 TO_INC FMCRs	Number of filter mode change records for which the filter mode has changed to include mode.
MLDv2 TO_EXC FMCRs	Number of filter mode change records for which the filter mode has changed to exclude mode.
MLDv2 ALLOW SLCRs	Number of source list change records for which the specified sources from where the data is to be received has changed.
MLDv2 BLOCK SLCRs	Number of source list change records for which the specified sources from where the data is to be received is to be blocked.

OSPF Statistics

The following commands display OSPF statistics.

Table 124. *OSPF Statistics Commands*

Command Syntax and Usage
`show ip ospf counters` Displays OSPF statistics. See page 243 for sample output. **Command mode:** All
`show ip ospf area counters` Displays OSPF area statistics. **Command mode:** All
`show ip ospf interface [`*<interface number>***`] counters`** Displays OSPF interface statistics. **Command mode:** All

OSPF Global Statistics

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

`show ip ospf counters`

Command mode: All

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

Nbr change stats:                 Intf change Stats:
  hello                   2            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 125. *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 125. *OSPF General Statistics (continued)*

Statistic	Description
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
Nbr Change Stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets must now be sent to the neighbor at intervals of `HelloInterval` seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.

Table 125. *OSPF General Statistics (continued)*

Statistic	Description
bad sequence	The sum total number of Database Description packets which have been received that either: a. Has an unexpected DD sequence number. b. Unexpectedly has the init bit set. c. Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
Intf Change Stats:	
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 125. *OSPF General Statistics (continued)*

Statistic	Description
Timers Kickoff:	
hello	The sum total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OPSF areas and interfaces.
retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
lsa ack	The sum total number of times the LSA `Ack` timer has been fired across all OSPF areas and interfaces.
dbage	The total number of times the data base age (`Dbage`) has been fired.
summary	The total number of times the Summary timer has been fired.
ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

OSPFv3 Statistics

The following commands display OSPFv3 statistics.

Table 126. *OSPFv3 Statistics Commands*

Command Syntax and Usage
show ipv6 ospf counters Displays OSPFv3 statistics. See page 243 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 127. *OSPFv3 General Statistics*

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
Discarded Pkts	The sum total of all OSPFv3 packets discarded.
Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.

Table 127. *OSPFv3 General Statistics (continued)*

Statistics	Description
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 (in the initial state of a neighbor conversation) across all OSPFv3 interfaces.
attempt	The total number of transitions into attempt state of neighboring routers across allOSPFv3 interfaces.
init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces.

Table 127. *OSPFv3 General Statistics (continued)*

Statistics	Description
exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.
Intf Change Stats:	
down	The total number of transitions into down state of all OSPFv3 interfaces.
loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.
backup	The total number of transitions into backup state of all OSPFv3 interfaces.
all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
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 128. *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 129. *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 transmitted or 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

The following commands display Management Processor statistics.

Table 130. *Management Processor Statistics Commands*

Command Syntax and Usage
show mp i2c Displays i2c statistics. **Command mode:** All
show mp memory Displays memory utilization statistics. **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 255. **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 266. **Command mode:** All
show mp thread Displays STEM thread statistics. This command is used by Technical Support personnel. **Command mode:** All
show mp udp-block Displays all UDP control blocks that are in use. To view a sample output, see page 267. **Command mode:** All
show processes cpu Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 267. **Command mode:** All
show processes cpu history Displays history of CPU utilization. To view a sample output, see page 269. **Command mode:** All

Packet Statistics

The following commands display Packet statistics.

Table 131. *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 255. **Command mode:** All
`clear mp packet logs` Clears all CPU packet statistics and logs. **Command mode:** Privileged EXEC

MP Packet Statistics

The following command displays MP packet statistics:

`show mp packet counters`

Command mode: All

```
CPU packet statistics at  8:21:54 Tue Jan  8, 2013

Packet rate:         Incoming            Outgoing
------------         --------            --------
1-second:                   8                   7
4-seconds:                  7                   5
64-seconds:                 4                   3

Packet counters:     Received                Sent
-----------------    --------                ----
Total packets:         109056              148761
Since bootup:          109056              148768
BPDUs:                   6415               19214
Cisco packets:              0                   0
ARP Requests:              15               10061
ARP Replies:             8545                  14
LACP packets:            3414                3420
IPv4 packets:           60130              116101
 ICMP Requests:             0                  21
 ICMP Replies:             21                   0
 IGMP packets:              0                   0
 PIM packets:               0                   0
 VRRP packets:              0                   0
 TCP  packets:          60088              116113
  FTP                       0                   0
  HTTP                      0                   0
  SSH                       3                   3
  TACACS                    0                   0
  TELNET                60095              116145
  TCP other                 0                   0
 UDP packets:              24                   9
  DHCP                      0                   0
  NTP                       0                   0
```

```
  RADIUS                    0                   0
  SNMP                      0                   0
  TFTP                      0                   0
  UDP other                24                   8
  RIP packets:              0                   1
  OSPF packets:             0                   0
  BGP packets:              0                   0
 IPv6 packets:              0                   0
 LLDP PDUs:              3987                6876
 FCoE FIP PDUs:             0                   0
 ECP PDUs:                  0                   0
 MgmtSock Packets:        919                 932
 Other:                 26549                   0

Packet Buffer Statistics:
-------------------------
 allocs:        265803
 frees:         265806
 failures:           0
 dropped:            0

 small packet buffers:
 ---------------------
   current:                 1
   max:                  1024
   threshold:             128
   hi-watermark:            3
   hi-water time:    3:39:12 Tue Jan  8, 2013

 medium packet buffers:
 ----------------------
   current:                 0
   max:                  2048
   threshold:               50
   hi-watermark:            1
   hi-water time:    3:37:12 Tue Jan  8, 2013

 jumbo packet buffers:
 ---------------------
   current:                 0
   max:                    16
   hi-watermark:            0

 pkt_hdr statistics:
 ---------------------
 current          :          0
 max              :       3072
 hi-watermark     :        180
```

Table 132. *Packet Statistics*

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.

Table 132. *Packet Statistics (continued)*

Statistics	Description
Packets Counters	
Total packets	Total number of packets received.
Since bootup	Total number of packets received and sent since the last switch reboot.
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received.
ARP packets	Total number of Address Resolution Protocol packets received.
IPv4 packets	Total number of IPv4 packets received and sent. Includes the following packet types: o IGMP o PIM o ICMP requests o ICMP replies
TCP packets	Total number of TCP packets received and sent. Includes the following packet types: o FTP o HTTP o SSH o TACACS+ o Telnet o Other
UDP packets	Total number of UDP packets received and sent. Includes the following packet types: o DHCP o NTP o RADIUS o SNMP o TFTP o 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.

Table 132. *Packet Statistics (continued)*

Statistics	Description
BGP packets	Total number of Border Gateway Protocol packets received and sent.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
ECP PDUs	Total number of Edge Control Protocol data units received and sent.
MgmtSock Packets	Total number of packets received and transmitted through the management port.
Other	Total number of other packets received.
Packet Buffer Statistics	
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
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.

Table 132. *Packet Statistics (continued)*

Statistics	Description
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of medium packet allocations supported.
threshold	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdr statistics	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

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 133. *Packet Statistics Log Options*

Command Syntax and Usage
show mp packet logs 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 260. **Command mode:** All
show mp packet logs rx Displays all packets logs received by the CPU. **Command mode:** All
show mp packet logs tx Displays all packet logs sent from the CPU. **Command mode:** All

Packet Log example

The following command displays all packet logs received by and sent from the CPU.

show mp packet logs all

Command mode: All

```
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 134. *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 260. **Command mode:** All
show mp packet last rx *<1-1000>* Displays a specified number of recent packet logs received by the CPU. **Command mode:** All
show mp packet last tx *<1-1000>* Displays a specified number of recent packet logs sent from the CPU. **Command mode:** All

Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

Table 135. *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. **Command mode:** All
show mp packet dump rx Displays all packet statistics and logs received by the CPU. **Command mode:** All
show mp packet dump tx Displays all packet statistics and logs sent from the CPU. **Command mode:** All

Logged Packet Statistics

The following command displays logged packets that have been received or sent, based on the specified filter:

show mp packet parse {rx|tx} *<parsing_option>*

The filter options are described in Table 136.

Table 136. *Packet Log Parsing Options*

Command Syntax and Usage
show mp packet parse {rx|tx} arp Displays only ARP packets logged. **Command mode:** All
show mp packet parse {rx|tx} bgp Displays only BGP packets logged. **Command mode:** All
show mp packet parse {rx|tx} bpdu Displays only BPDUs logged. **Command mode:** All
show mp packet parse {rx|tx} cisco Displays only Cisco packets (BPDU/CDP/UDLD) logged. **Command mode:** All
show mp packet parse {rx|tx} dhcp Displays only DHCP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ecp Displays only ECP packets logged. **Command mode:** All
show mp packet parse {rx|tx} fcoe Displays only FCoE FIP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} ftp Displays only FTP packets logged. **Command mode:** All
show mp packet parse {rx|tx} http Displays only HTTP packets logged. **Command mode:** All

Table 136. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} https Displays only HTTPS packets logged. **Command mode:** All
show mp packet parse {rx|tx} icmp Displays only ICMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} igmp Displays only IGMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ip-addr *<IPv4_address>* Displays only logged packets with the specified IPv4 address. **Command mode:** All
show mp packet parse {rx|tx} ipv4 Displays only IPv4 packets logged. **Command mode:** All
show mp packet parse {rx|tx} ipv6 Displays only IPv6 packets logged. **Command mode:** All
show mp packet parse {rx|tx} lacp Displays only LACP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} lldp Displays only LLDP PDUs logged. **Command mode:** All
show mp packet parse {rx|tx} mac *<MAC_address>* Displays only logged packets with the specified MAC address. **Command mode:** All
show mp packet parse {rx|tx} mgmtsock Displays only packets logged on management ports. **Command mode:** All
show mp packet parse {rx|tx} ntp Displays only NTP packets logged. **Command mode:** All

Table 136. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} ospf Displays only OSPF packets logged. **Command mode:** All
show mp packet parse {rx|tx} other Displays logs of all packets not explicitly selectable. **Command mode:** All
show mp packet parse {rx|tx} pim Displays only PIM packets logged. **Command mode:** All
show mp packet parse {rx|tx} port *<port_number>* Displays only logged packets with the specified port. **Command mode:** All
show mp packet parse {rx|tx} radius Displays only RADIUS packets logged. **Command mode:** All
show mp packet parse {rx|tx} rarp Displays only Reverse-ARP packets. **Command mode:** All
show mp packet parse {rx|tx] raw Displays raw packet buffer in addition to headers. **Command mode:** All
show mp packet parse {rx|tx} rip Displays only RIP packets logged. **Command mode:** All
show mp packet parse {rx|tx} snmp Displays only SNMP packets logged. **Command mode:** All
show mp packet parse {rx|tx} ssh Displays only SSH packets logged. **Command mode:** All
show mp packet parse {rx|tx} tacacs Displays only TACACS packets logged. **Command mode:** All

Table 136. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} tcp Displays only TCP packets logged. **Command mode:** All
show mp packet parse {rx|tx} tcpother Displays only TCP other-port packets logged. **Command mode:** All
show mp packet parse {rx|tx} telnet Displays only TELNET packets logged. **Command mode:** All
show mp packet parse {rx|tx} tftp Displays only TFTP packets logged. **Command mode:** All
show mp packet parse {rx|tx} udp Displays only UDP packets logged. **Command mode:** All
show mp packet parse {rx|tx} udpother Displays only UDP other-port packets logged. **Command mode:** All
show mp packet parse {rx|tx} vlan *<VLAN_number>* Displays only logged packets with the specified VLAN. **Command mode:** All
show mp packet parse {rx|tx} vrrp Displays only VRRP logged packets. **Command mode:** All

TCP Statistics

The following command displays TCP statistics:

`show mp tcp-block`

Command mode: All

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

Mgmt Ports:
------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 172.31.38.107:http      *:*                     LISTEN
tcp        0      0 172.31.38.107:telnet    *:*                     LISTEN
tcp        0      0 *:11000                 *:*                     LISTEN
tcp        0   1274 172.31.38.107:telnet    172.31.37.42:55866      ESTABLISHED
```

Table 137. *MP Specified TCP Statistics*

Statistics	Description
`14835bd8`	Memory
`0.0.0.0`	Destination IP address
`0`	Destination port
`172.31.38.107`	Source IP
`80`	Source port
`listen MGT1 up`	State

UDP Statistics

The following command displays UDP statistics:

`show mp udp-block`

Command mode: All

```
Data Ports:
--------------------------------------------------------------------
All UDP allocated control blocks:
   68:  listen
  161:  listen
  500:  listen
  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 commands display CPU utilization statistics:

`show mp cpu`

Command mode: All

```
       CPU utilization            Highest     Thread                Time
------------------------------   -------   ----------    -------------------------
cpuUtil1Second:             3%      83%     58 (I2C )    12:02:14 Fri Oct 14, 2011
cpuUtil4Seconds:            5%
cpuUtil64Seconds:           5%
```

Table 138. *CPU Statistics*

Statistics	Description
cpuUtil1Second	The use of MP CPU over 1 second. It shows the percentage, highest rate, thread, and time the highest utilization occurred.
cpuUtil4Seconds	The use of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The use of MP CPU over 64 seconds. It shows the percentage.
Highest	The highest percent of CPU use.
Thread	The thread ID and name of the thread that caused the highest CPU use.
Time	The time when the highest CPU use was reached.

show processes cpu

Command mode: All

```
CPU Utilization at  8:25:55 Tue Jan  8, 2013

Total CPU Utilization: For 1 second: 2.92%
                       For 5 second: 3.38%
                       For 1 minute: 7.88%
                       For 5 minute: 8.93%

Highest CPU Utilization: thread   2 (STP ) at  6:44:56 Tue Jan  8, 2013

------------------------------------------------------------------------
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%      0.05%      0.10%      0.10%       idle
  3      MFDB       0.00%      0.00%      5.06%      5.22%       idle
  4      TND        0.00%      0.00%      0.00%      0.00%       idle
  5      CONS       0.00%      0.00%      0.00%      0.15%  suspended
  6      TNET       0.11%      0.58%      0.17%      0.27%    running
  7      TNET       0.00%      0.00%      0.00%      0.00%       idle
  8      TNET       0.00%      0.00%      0.00%      0.00%       idle
  9      TNET       0.00%      0.00%      0.00%      0.00%       idle
 10      LOG        0.00%      0.00%      0.00%      0.00%       idle
 11      TRAP       0.00%      0.00%      0.00%      0.00%       idle
 13      NTP        0.00%      0.00%      0.00%      0.00%       idle
 14      IP         0.04%      0.04%      0.06%      0.06%       idle
 17      IP         0.01%      0.08%      0.04%      0.04%       idle
 18      RIP        0.00%      0.00%      0.00%      0.00%       idle
 19      AGR        0.00%      0.00%      0.00%      0.00%       idle
 20      EPI        0.16%      0.27%      0.12%      0.10%   runnable
 22      PORT       0.00%      0.00%      0.00%      0.00%       idle
 24      BGP        0.18%      0.04%      0.00%      0.00%       idle
 32      SCAN       0.00%      0.00%      0.00%      0.00%       idle
 34      OSPF       0.20%      0.04%      0.02%      0.01%       idle
 36      SNMP       0.00%      0.00%      0.00%      0.00%       idle
 37      SNMP       0.00%      0.00%      0.00%      0.00%       idle
 38      SNMP       0.00%      0.00%      0.00%      0.00%       idle
 40      SSHD       0.00%      0.00%      0.00%      0.00%       idle
...
120      VDPT       0.00%      0.00%      0.00%      0.00%       idle
124      HIST       0.00%      0.00%      0.00%      0.00%   runnable
128      NORM       0.00%      0.00%      0.00%      0.00%       idle
129      NORM       0.00%      0.00%      0.00%      0.00%       idle
130      DONE       0.00%      0.00%      0.00%      0.00%       idle
```

Table 139. *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.

Table 139. *CPU Statistics*

Statistics	Description
5Min	The percent of CPU use over 5 minutes.
Status	The status of the process.

CPU Statistics History

The following command display a history of CPU use statistics:

`show processes cpu history`

Command mode: All

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

Access Control List Statistics

The following commands display and change ACL statistics.

Table 140. *ACL Statistics Commands*

Command Syntax and Usage
show access-control counters Displays all ACL statistics. For output sample, see page 271. **Command mode:** All
show access-control list *<1-256>* **counters** Displays the Access Control List Statistics for a specific ACL. **Command mode:** All
show access-control list6 *<1-128>* **counters** Displays the IPv6 ACL statistics for a specific ACL. **Command mode:** All
show access-control macl *<1-128>* **counters** Displays the ACL statistics for a specific management ACL (MACL). **Command mode:** All
show access-control meter *<1-127>* **counters** Displays ACL meter statistics. For output sample, see page 271. **Command mode:** All
show access-control vmap *<1-128>* **counters** Displays VLAN Map statistics for the selected VMAP. For details, see page 271. **Command mode:** All
clear access-control list {*<1-256>***|all} counters** Clears ACL statistics. **Command mode:** Privileged EXEC
clear access-control list6 {*<1-128>***|all}** Clears IPv6 ACL statistics. **Command mode:** Privileged EXEC
clear access-control meter *<1-127>* **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
```

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
```

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

```
FCF-keepalives statistics:
FCF 54:7f:ee:8f:d4:2a keepalives received : 62
FCOE statistics:
FCFAdded:                   5   FCFRemoved:                  1
FCOEAdded:                  81  FCOERemoved:                 24
```

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

Table 141. *FCoE Statistics*

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: All

SNMP Statistics

The following command displays SNMP statistics:

`show snmp-server counters`

Command mode: All except User EXEC

```
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 142. *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 142. *SNMP Statistics (continued)*

Statistic	Description
snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpOutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue.`
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value `read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.

Table 142. *SNMP Statistics (continued)*

Statistic	Description
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is *too big*.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName`.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpOutReadOnlys	Not in use.

Table 142. *SNMP Statistics (continued)*

Statistic	Description
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the 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

Lenovo N/OS uses NTP (Network Timing Protocol) version 3 to synchronize the switch's internal clock with an atomic time calibrated NTP server. With NTP enabled, the switch can accurately update its internal clock to be consistent with other devices on the network and generates accurate syslogs.

The following command displays NTP statistics:

`show ntp counters`

Command mode: All

```
NTP statistics:
        Primary Server:
                Requests Sent:               17
                Responses Received:          17
                Updates:                     1
        Secondary Server:
                Requests Sent:               0
                Responses Received:          0
                Updates:                     0

        Last update based on response from primary/secondary server.
        Last update time: 18:04:16 Tue Jul 13, 2010
        Current system time: 18:55:49 Tue Jul 13, 2010
```

Table 143. *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 143. *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 command was issued.

The following command displays information about NTP associated peers:

`show ntp associations`

Command mode: All

```
 address         ref clock          st    when(s)   offset(s)
*12.200.151.18   198.72.72.10       3     35316     -2
*synced, #unsynced
```

Table 144. *NTP Associations*

Field	Description
address	Peer address
ref clock	Peer reference clock address
st	Peer stratum
when(s)	Time in seconds since the latest NTP packet was received from the peer
offset(s)	Offset in seconds between the peer clock and local clock

SLP Statistics

The following table displays SLP statistics commands:

Table 145. *SLP Statistics Commands*

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

Command mode: All

```
CPU Utilization at 12:13:08 Thu Mar 12, 2015

Total CPU Utilization: For 1 second: 0.06%
                       For 5 second: 0.33%
                       For 1 minute: 0.12%
                       For 5 minute: 0.11%

Highest CPU Utilization: thread  16 (IP  ) at 14:12:23 Wed Feb 25, 2015

--------------------------------------------------------------------
Thread  Thread                    Utilization                  Status
  ID     Name        1sec       5sec       1Min       5Min
--------------------------------------------------------------------
  1      STEM       0.00%      0.00%      0.00%      0.00%       idle
  2      STP        0.00%      0.00%      0.00%      0.00%       idle
  3      MFDB       0.00%      0.00%      0.00%      0.00%       idle
  4      TND        0.00%      0.00%      0.00%      0.00%       idle
  5      CONS       0.01%      0.02%      0.00%      0.01%    running
  6      TNET       0.00%      0.00%      0.00%      0.00%       idle
  7      TNET       0.00%      0.00%      0.00%      0.00%       idle
  8      TNET       0.00%      0.00%      0.00%      0.00%       idle
  9      TNET       0.00%      0.00%      0.00%      0.00%       idle
 10      LOG        0.00%      0.00%      0.00%      0.00%       idle
 11      TRAP       0.00%      0.00%      0.00%      0.00%       idle
 12      NTP        0.00%      0.00%      0.00%      0.00%       idle
 13      RMON       0.00%      0.00%      0.00%      0.00%       idle
 16      IP         0.00%      0.01%      0.01%      0.01%       idle
 18      AGR        0.00%      0.00%      0.00%      0.00%       idle
 19      EPI        0.00%      0.00%      0.00%      0.00%       idle
 20      PORT       0.00%      0.00%      0.00%      0.00%       idle
 25      MGMT       0.01%      0.01%      0.01%      0.02%       idle
 28      SNMP       0.00%      0.00%      0.01%      0.00%       idle
 29      SNMP       0.00%      0.00%      0.00%      0.00%       idle
 31      SSHD       0.00%      0.00%      0.00%      0.00%       idle
 33      TEAM       0.00%      0.00%      0.00%      0.00%       idle
 34      I2C        0.00%      0.00%      0.00%      0.00%       idle
 35      LACP       0.01%      0.25%      0.04%      0.02%       idle
 36      SFP        0.00%      0.00%      0.00%      0.00%       idle
 37      L3HS       0.00%      0.00%      0.00%      0.00%       idle
 38      HLNK       0.00%      0.00%      0.00%      0.00%       idle
 39      LLDP       0.00%      0.00%      0.01%      0.02%       idle
 40      IPV6       0.00%      0.01%      0.00%      0.00%       idle
...
```

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

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

Chapter 4. Configuration Commands

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

Table 146. *General Configuration Commands*

Command Syntax and Usage
`show running-config [diff]` Dumps current configuration to a script file. The `diff` option displays only the running configuration changes that have been applied but not saved to flash memory. For details, see page 550. **Command mode:** All except User EXEC
`copy running-config backup-config` Copy the current (running) configuration from switch memory to the `backup-config` partition. For details, see page 551. **Command mode:** All except User EXEC
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the `startup-config` partition. **Command mode:** All except User EXEC
`copy running-config {ftp|sftp|tftp} [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:** All except User EXEC
`copy {ftp|sftp|tftp} 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 552. **Command mode:** All except User EXEC

Table 146. *General Configuration Commands*

Command Syntax and Usage
copy {sftp|tftp} {ca-cert|host-key|host-cert|public-key} [data-port|extm-port|mgt-port] Imports interface used by NIST certified test laboratories for USGv6 (NIST SP 500-267) certification purposes. Required for RSA digital signature authentication verification during IKEv2 interoperability testing. Uses TFTP or SFTP to import: o `ca-cert`: Certificate Authority root certificate o `host-key`: host private key o `host-cert`: host public key o `public-key:` client public key o `data-port:` data port o `extm-port:` external management port o `mgt-port:` management port **Command mode:** All except User 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 one of the following commands:

```
CN 4093# copy running-config startup-config
```

or

```
CN 4093# write
```

Note: The `write` command doesn't prompt the user for confirmation.

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see "Selecting a Configuration Block" on page 577.

System Configuration

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

Table 147. *System Configuration Commands*

Command Syntax and Usage
`[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] boot strict enable` Enables or disables switch operation in security strict mode. When `enabled`, the authentication and privacy protocols and algorithms of the device are compliant with NIST SP-800-131A, with non-compliant protocols and algorithms disabled. Setting will be applied and device will be reset to default factory configuration after reboot. The default setting is `disabled`. **Note:** Ensure NIST Strict compliance is enabled on the Chassis Management Module before enabling Strict mode operation on the device. **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
`line console length` *<0-300>* Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is `28`. **Command mode:** Global configuration
`no line console` Sets `line console length` to the default value of `28`. **Command mode:** Global configuration
`line vty length` *<0-300>* Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is `28`. **Command mode:** Global configuration

Table 147. *System Configuration Commands (continued)*

Command Syntax and Usage
no line vty Sets `line vty length` to the default value of `28`. **Command mode:** Global configuration
system date *<yyyy> <mm> <dd>* Prompts the user for the system date. The date retains its value when the switch is reset. **Command mode:** Global configuration
[no] system daylight Enables or disables daylight saving time in the system clock. When `enabled`, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is `disabled`. **Command mode:** Global configuration
[no] system dhcp [extm|mgt] Enables or disables Dynamic Host Control Protocol for setting the IP address on the selected interface. When `enabled`, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`. **Command mode:** Global configuration
[no] system dhcp {hostname|syslog} Enables or disables hostname or log server options support for DHCP/BOOTP client. **Command mode:** Global configuration
system idle *<0-60>* Sets the idle timeout for CLI sessions in minutes. A value of 0 disables system idle. The default value is `10` minutes. **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
[no] system notice *<maximum 1024 character multi-line login notice> <'.' to end>* Enables or disables the display of a login notice immediately before the "Enter password:" prompt. This notice can contain up to 1024 characters and new lines. **Command mode:** Global configuration

Table 147. *System Configuration Commands (continued)*

Command Syntax and Usage
`[no] system packet-logging` Enables or disables logging of packets that come to the CPU. The default setting is `enabled`. **Command mode:** Global configuration
`[no] system reset-control` Enables or disables the reset control flag. When `enabled`, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. **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
`terminal-length` *<0-300>* Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding `line vty length` or `line console length` value in effect at login. **Command mode:** All
`show boot strict` Displays the current security strict mode status. **Command mode:** Global configuration
`show system` Displays the current system parameters. **Command mode:** All

System 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 148. *Error Disable Configuration Commands*

Command Syntax and Usage
`[no] errdisable recovery` Globally enables or disables automatic error-recovery for error-disabled ports. The default setting is `disabled`. **Note**: Each port must have error-recovery enabled to participate in automatic error recovery. **Command mode:** Global configuration
`errdisable timeout` *<30-86400>* Configures the error-recovery timeout, in seconds. After the timer expires, the switch attempts to re-enable the port. The default value is `300` seconds. **Note**: When you change the timeout value, all current error-recovery timers are reset. **Command mode:** Global configuration
`show errdisable` Displays the current system Error Disable configuration. **Command mode:** All

Link Flap Dampening Configuration

The Link Flap Dampening feature allows the switch to automatically disable a port if too many link flaps (link up/link down) are detected on the port during a specified time interval. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed.

Table 149. *Link Flap Dampening Configuration Options*

Command Syntax and Usage
`[no] errdisable link-flap enable` Enables or disables Link Flap Dampening. **Command mode**: Global configuration
`errdisable link-flap max-flaps` *<1-100>* Configures the maximum number of link flaps allowed in the configured time period. The default value is `5`. **Command mode**: Global configuration
`errdisable link-flap time` *<5-500>* Configures the time period, in seconds. The default value is `30` seconds. **Command mode**: Global configuration
`show errdisable link-flap` Displays the current Link Flap Dampening parameters. **Command mode**: All

System Host Log Configuration

The following table displays System Host Log configuration commands.

Table 150. *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. The default is 7, which means log all severity levels. **Command mode**: Global configuration
[no] logging console Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. The default setting is enabled. **Command mode:** Global configuration
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. The default is 7, which means log all severity levels. **Command mode:** Global configuration
no logging console severity Disables delivering syslog messages to the console based on severity. **Command mode:** Global configuration
logging host *<1-2>* **address** *<IP address>* **[data-port|extm-port|mgt-port]** Sets the IPv4 address of the first or second syslog host. **Command mode:** Global configuration
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
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

Table 150. *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
no logging host *<1-2>* Removes the specified syslog host. **Command mode:** Global configuration
[no] logging log {all|*<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
[no] logging pdrop enable Enables or disables packet drop logging. By default, the switch generates these messages once every 30 minutes. **Command mode:** Global configuration
logging pdrop interval *<0-30>* Sets the packet drop logging interval, in minutes. The default value is 30. **Command mode:** Global configuration
[no] logging synchronous [level *<0-7>* **| all]** Enables or disables synchronous logging messages. When **enabled**, logging messages are displayed asynchronously. The level parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. All displays all messages asynchronously, regardless the severity level. The default setting is 2. **Command mode:** Global configuration
logging source-interface loopback *<1-5>* Sets the loopback interface number for syslogs. **Command mode:** Global configuration

Table 150. *Host Log Configuration Commands*

Command Syntax and Usage
`no logging source-interface loopback` Removes the loopback interface for syslogs. **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 47. 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 151. *SSH Server Configuration Commands*

Command Syntax and Usage
[no] ssh enable Enables or disables the SSH server. **Command mode:** Global configuration
ssh generate-host-key Generate the RSA host key. **Command mode:** Global configuration
ssh maxauthattempts *<1-20>* Sets the maximum number of SSH authentication attempts. The default value is 2. **Command mode:** Global configuration
no ssh maxauthattempts Resets the maximum number of SSH authentication attempts to its default value of 2. **Command mode:** Global configuration
ssh port *<TCP port number>* Sets the SSH server port number. The default port number is 22. **Command mode:** Global configuration
no ssh port Resets the SSH server port to the default port number 22. **Command mode:** Global configuration
ssh public-key index *<1-100>* **{adduser|deluser} username** *<user name>* Assigns another user name for existing public keys or removes a user name. **Command mode:** Global configuration
[no] ssh scp-enable Enables or disables the SCP apply and save. **Command mode:** Global configuration
ssh scp-password Set the administration password for SCP access. **Command mode:** Global configuration

Table 151. *SSH Server Configuration Commands*

Command Syntax and Usage
show ssh Displays the current SSH server configuration. **Command mode:** All
show ssh-clienthostkey {address *<SFTP server IP address>***|all}** Displays the current SFTP/SSH host key configuration. o `address`: Displays a specific SFTP/SSH host key o `all`: Displays all SFTP/SSH host keys **Commands mode:** All
show ssh-clientpubkey {all|index *<1-100>***|username** *<user name>***}** Displays the current SSH public key configuration. o `all`: Displays all SSH public keys o `index`: Displays a specific SSH public key o `username`: Displays all the SSH public keys of a particular user **Command mode:** All
clear ssh-clienthostkey {address *<SFTP server IP address>***|all}** Clears stored SFTP/SSH host key configuration. o `address`: Clears a specific SFTP/SSH host key o `all`: Clears all SFTP/SSH host keys **Command mode:** All except User EXEC
clear ssh-clientpubkey {all|index *<1-100>***|username** *<user name>***}** Clears stored SSH public key configuration. o `all`: Clears all SSH public keys o `index`: Clears a specific SSH public key o `username`: Clears a particular username from all the SSH public keys **Command mode:** All except User EXEC

RADIUS Server Configuration

The following table displays RADIUS Server configuration commands.

Table 152. *RADIUS Server Configuration Commands*

Command Syntax and Usage
[no] radius-server backdoor Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is `disabled`. To obtain the RADIUS backdoor password for your switch, contact your Service and Support line. **Command mode:** Global configuration
[no] radius-server enable Enables or disables the RADIUS server. **Command mode:** Global configuration
[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
[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 *<hostname or IP address>* **[key** *<1-32 characters>***]** This is the primary shared secret between the switch and the RADIUS server(s). The `key` option sets the RADIUS server secret key. **Command mode:** Global configuration
no radius-server primary-host [key] Removes the primary RADIUS server. The `key` option removes only the RADIUS server secret key. **Command mode:** Global configuration
radius-server retransmit *<1-3>* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is `3` requests. **Command mode:** Global configuration

Table 152. *RADIUS Server Configuration Commands*

Command Syntax and Usage
radius-server secondary-host *<hostname or IP address>* **[key** *<1-32 characters>***]** This is the secondary shared secret between the switch and the RADIUS server(s). The key option sets the RADIUS server secret key. **Command mode:** Global configuration
no radius-server secondary-host [key] Removes the secondary RADIUS server. The key option removes only the RADIUS server secret key. **Command mode:** Global configuration
[no] radius-server secure-backdoor Enables or disables the RADIUS backdoor using secure password for Telnet/SSH/HTTP/HTTPS. **Note:** This command does not apply when RADIUS backdoor is enabled. **Command mode:** Global configuration
radius-server timeout *<1-10>* Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds. **Command mode:** Global configuration
ip radius source-interface loopback *<1-5>* Sets the RADIUS source loopback interface. **Command mode:** Global configuration
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 153. *TACACS+ Server Configuration Commands*

Command Syntax and Usage
`[no] tacacs-server accounting-enable` Enables or disables TACACS+ accounting. **Command mode:** Global configuration
`[no] tacacs-server attempts` *<1-10>* Sets the number of failed login attempts before disconnecting the user. The default is `2` attempts. **Command mode:** Global configuration
`[no] tacacs-server 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
`tacacs-server chpassp` *<1-32 characters>* Defines the password for the primary TACACS+ server. **Command mode:** Global configuration

Table 153. *TACACS+ Server Configuration Commands (continued)*

Command Syntax and Usage
`tacacs-server chpasss` *<1-32 characters>* Defines the password for the secondary TACACS+ server. **Command mode:** Global configuration
`[no] tacacs-server command-authorization` Enables or disables TACACS+ command authorization. **Command mode:** Global configuration
`[no] tacacs-server command-logging` Enables or disables TACACS+ command logging. **Command mode:** Global configuration
`[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: o `Restricted`: Only the username is sent to the specified TACACS+ server. o `No-truncate`: The entire login string is sent to the TACACS+ server. **Command mode:** Global configuration
`[no] tacacs-server enable` Enables or disables the TACACS+ server. By default, the server is `disabled`. **Command mode:** Global configuration
`[no] tacacs-server enable-bypass` Enables or disables the enable-bypass for administrator privilege. By default, enable-bypass is `enabled`. **Command mode:** Global configuration
`[no] tacacs-sercer encryption-enable` Enables or disables encryption for TACACS+ traffic packets. **Command mode:** Global configuration
`[no] tacacs-server password-change` Enables or disables TACACS+ password change. The default value is `disabled`. **Command mode:** Global configuration

Table 153. *TACACS+ Server Configuration Commands (continued)*

Command Syntax and Usage
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
[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
[no] tacacs-server primary-host *<IP address>* Defines the primary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server primary-host *<IP address>* **key** *<1-32 characters>* This is the primary shared secret key between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] tacacs-server privilege-mapping Enables or disables TACACS+ privilege-level mapping. The default value is disabled. **Command mode:** Global configuration
tacacs-server retransmit *<1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests. **Command mode:** Global configuration
[no] tacacs-server secondary-host *<IP address>* Defines the secondary TACACS+ server address. **Command mode:** Global configuration
[no] tacacs-server secondary-host *<IP address>* **key** *<1-32 characters>* This is the secondary shared secret key between the switch and the TACACS+ server(s). **Command mode:** Global configuration

Table 153. *TACACS+ Server Configuration Commands (continued)*

Command Syntax and Usage
`[no] tacacs-server secure-backdoor` Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default is `disabled`. **Command mode:** Global configuration
`tacacs-server timeout` *<4-15>* Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is `5` seconds. **Command mode:** Global configuration
`[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
`ip tacacs-server source-interface loopback` *<1-5>* Sets the TACACS+ source loopback interface. **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 154. *LDAP Server Configuration Commands*

Command Syntax and Usage
ldap-server attribute username *<1-128 characters>* Sets a customized LDAP user attribute. The defaul value is `uid`. **Note:** The user attribute needs to be set to `cn` if LDAP server is MS active directory. **Command mode:** Global configuration
no ldap-server attribute [username] Sets LDAP attributes back to their default values. The `username` option sets the LDAP user attribute back to its default value of `uid`. **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`. **Note:** To obtain the LDAP back door password for your CN4093, contact your Service and Support line. **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 enable Enables or disables the LDAP server. **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
[no] ldap-server primary-host *<IP address>* Sets the primary LDAP server address. **Command mode:** Global configuration

Table 154. *LDAP Server Configuration Commands (continued)*

Command Syntax and Usage
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
[no] ldap-server secondary-host *<IP address>* Sets the secondary LDAP server address. **Command mode:** Global configuration
ldap-server timeout *<4-15>* Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds. **Command mode:** Global configuration
show ldap-server Displays the current LDAP server parameters. **Command mode:** All

NTP Server Configuration

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

Table 155. *NTP Server Configuration Commands*

Command Syntax and Usage
`[no] ntp authenticate` Enables or disables NTP authentication. When authentication is `enabled`, the switch transmits NTP packets with the MAC address appended. The default setting is `disabled`. **Command mode:** Global configuration
`[no] ntp enable` Enables or disables the NTP synchronization service. **Command mode:** Global configuration
`ntp interval` *<5-44640>* Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server. The default value is `1440`. **Command mode:** Global configuration
`ntp offset` *<0-86400>* Configures the minimum offset in seconds between the switch clock and the NTP server that triggers a system log message. The default value is `300`. **Command mode:** Global configuration
`no ntp offset` Resets the NTP offset to the default `300` seconds value. **Command mode:** Global configuration
`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

Table 155. *NTP Server Configuration Commands*

Command Syntax and Usage
ntp primary-server *<IP address>* **[data-port|extm-port|mgt-port]** 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: o data port (**data**) o external management port (**extm**) o internal management port (**mgt**) **Command mode:** Global configuration
no ntp primary-server Removes the primary NTP server address. **Command mode:** Global configuration
ntp secondary-server *<IP address>* **[data-port|extm-port|mgt-port]** 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: o data port (**data**) o external management port (**extm**) o internal management port (**mgt**) **Command mode:** Global configuration
no ntp secondary-server Removes the secondary NTP server address. **Command mode:** Global configuration
ntp ipv6 primary-server *<IPv6 address>* **[data-port|extm-port|mgt-port]** 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: o data port (**data**) o external management port (**extm**) o internal management port (**mgt**) **Command mode:** Global configuration
no ntp ipv6 primary-server Removes the IPv6 primary NTP server address. **Command mode:** Global configuration

Table 155. *NTP Server Configuration Commands*

Command Syntax and Usage
ntp ipv6 secondary-server *<IPv6 address>* **[data-port|extm-port|mgt-port]** 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: o data port (**data**) o external management port (**extm**) o internal management port (**mgt**) **Command mode:** Global configuration
no ntp ipv6 secondary-server Removes the IPv6 secondary NTP server address. **Command mode:** Global configuration
[no] ntp sync-logs Enables or disables informational logs for NTP synchronization failures. The default setting is `enabled`. **Command mode:** Global configuration
[no] ntp source loopback *<1-5>* Sets the NTP source loopback interface. **Command mode:** Global configuration
[no] ntp trusted-key *<1-65534>* Adds or removes an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code. **Command mode:** Global configuration
show ntp Displays the current NTP service settings. **Command mode:** All

NTP MD5 Key Commands

The following table displays NTP MD5 Key configuration commands.

Table 156. *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

Lenovo N/OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

An SNMP agent is a software process on the managed device that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or to modify.

SNMP parameters that can be modified include:

- System name
- System location
- System contact
- Use of the SNMP system authentication trap function
- Read community string
- Write community string
- Trap community strings

Table 157. *System SNMP Commands*

Command Syntax and Usage
`[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 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 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

Table 157. *System SNMP Commands*

Command Syntax and Usage
[no] snmp-server link-trap *<port alias or number>* **enable** Enables or disables the sending of SNMP link up and link down traps for the specified port. The default setting is `enabled`. **Command mode:** Global configuration
[no] snmp-server location *<1-64 characters>* Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode:** Global configuration
[no] snmp-server 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 read-community *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is `public`. **Command mode:** Global configuration
[no] snmp-server read-community-additional *<1-32 characters>* Adds or removes an additional SNMP read community string. Up to 7 additional read community strings are supported. **Command mode:** Global configuration
snmp-server timeout *<1-30>* Sets the timeout value for the SNMP state machine, in minutes. **Command mode:** Global configuration
[no] snmp-server trap-source {<*interface number*>**|loopback** *<1-5>***}** Configures the source interface for SNMP traps. **Command mode:** Global configuration
snmp-server write-community *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is `private`. **Command mode:** Global configuration

Table 157. *System SNMP Commands*

Command Syntax and Usage
`[no] snmp-server write-community-additional` *<1-32 characters>* Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported. **Command mode:** Global configuration
`show snmp-server` Displays the current SNMP configuration. **Command mode:** All

SNMPv3 Configuration

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

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

For more details on the SNMPv3 architecture please refer to RFC3411 to RFC3418.

Table 158. *SNMPv3 Configuration Commands*

Command Syntax and Usage
`snmp-server access` *<1-32>* This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view command options, see page 311. **Command mode:** Global configuration
`snmp-server community` *<1-16>* The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view command options, see page 313. **Command mode:** Global configuration
`snmp-server group` *<1-17>* A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view command options, see page 312. **Command mode:** Global configuration

Table 158. *SNMPv3 Configuration Commands (continued)*

`snmp-server notify` *<1-16>* A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view command options, see page 316. **Command mode:** Global configuration
`snmp-server target-address` *<1-16>* This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view command options, see page 314. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view command options, see page 315. **Command mode:** Global configuration
`snmp-server user` *<1-17>* This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view command options, see page 309. **Command mode:** Global configuration
`snmp-server version {v1v2v3|v3only}` This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. The default value is `v1v2v3`. **Command mode:** Global configuration
`snmp-server view` *<1-128>* This command allows you to create different MIB views. To view command options, see page 310. **Command mode:** Global configuration
`show snmp-server v3` Displays the current SNMPv3 configuration. **Command mode:** All

User Security Model Configuration

You can make use of a defined set of user identities using this Security Model. An SNMP engine must have the knowledge of applicable attributes of a user.

These commands help you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

Table 159. *User Security Model Configuration Commands*

Command Syntax and Usage
snmp-server user *<1-17>* **authentication-protocol {md5|sha|none} authentication-password** *<password value>* This command allows you to configure the authentication protocol and password. The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96 for compatibility mode, HMAC-SHA-96 for security strict mode, or none. The default algorithm is `none`. `MD5` authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility. When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication. **Command mode:** Global configuration
snmp-server user *<1-17>* **name** *<1-32 characters>* This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch. **Command mode:** Global configuration
snmp-server user *<1-17>* **privacy-protocol {aes|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), `aes` (AES-128 Advanced Encryption Standard Protocol) or `none`. If you specify `des` as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). In security strict mode, if you do not select SNMPv3 account backward compatibility, make sure to disable `des` privacy protocol. If you specify `aes` as the privacy protocol, make sure that you have selected HMAC-SHA-256 authentication protocol. If you select `none` as the authentication protocol, you will get an error message. You can create or change the privacy password. **Command mode:** Global configuration

Table 159. *User Security Model Configuration Commands*

Command Syntax and Usage
no snmp-server user *<1-17>* Deletes the USM user entries. **Command mode:** Global configuration
show snmp-server v3 user *<1-17>* Displays the USM user entries. **Command mode:** All

SNMPv3 View Configuration

Note that the first five default `vacmViewTreeFamily` entries cannot be removed, and their names cannot be changed.

Table 160. *SNMPv3 View Configuration Commands*

Command Syntax and Usage
[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>* **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
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 161. *View-based Access Control Model Commands*

Command Syntax and Usage
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>* **name** *<1-32 characters>* Defines the name of the group. **Command mode:** Global configuration
snmp-server access *<1-32>* **notify-view** *<1-32 characters>* Defines a notify view name that allows you notify access to the MIB view. **Command mode:** Global configuration
snmp-server access *<1-32>* **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>* **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 161. *View-based Access Control Model Commands (continued)*

Command Syntax and Usage
snmp-server access *<1-32>* **security {usm|snmpv1|snmpv2}** Allows you to select the security model to be used. **Command mode:** Global configuration
snmp-server access *<1-32>* **write-view** *<1-32 characters>* Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode:** Global configuration
no snmp-server access *<1-32>* Deletes the View-based Access Control entry. **Command mode:** Global configuration
show snmp-server v3 access *<1-32>* Displays the View-based Access Control configuration. **Command mode:** All

SNMPv3 Group Configuration

The following table displays SNMPv3 Group configuration commands.

Table 162. *SNMPv3 Group Configuration Commands*

Command Syntax and Usage
snmp-server group *<1-17>* **group-name** *<1-32 characters>* The name for the access group as defined in the following command: `snmp-server access` *<1-32>* `name` *<1-32 characters>* on page 309. **Command mode:** Global configuration
snmp-server group *<1-17>* **security {usm|snmpv1|snmpv2}** Defines the security model. **Command mode:** Global configuration
snmp-server group *<1-17>* **user-name** *<1-32 characters>* Sets the user name as defined in the following command on page 309: `snmp-server user` *<1-17>* `name` *<1-32 characters>* **Command mode:** Global configuration
no snmp-server group *<1-17>* Deletes the `vacmSecurityToGroup` entry. **Command mode:** Global configuration
show snmp-server v3 group *<1-17>* Displays the current `vacmSecurityToGroup` configuration. **Command mode:** All

SNMPv3 Community Table Configuration

These commands are used for configuring the community table entry. The configured entry is stored in the community table list in the SNMP engine. This table is used to configure community strings in the Local Configuration Datastore (LCD) of SNMP engine.

Table 163. *SNMPv3 Community Table Configuration 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 309: `snmp-server user` *<1-17>* `name` *<1-32 characters>* **Command string:** Global configuration
snmp-server community *<1-16>* **tag** *<1-255 characters>* Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** Global configuration
snmp-server community *<1-16>* **user-name** *<1-32 characters>* Defines a readable string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
no snmp-server community *<1-16>* Deletes the community table entry. **Command mode:** Global configuration
show snmp-server v3 community *<1-16>* Displays the community table configuration. **Command mode:** All

SNMPv3 Target Address Table Configuration

These commands are used to configure the target transport entry. The configured entry is stored in the target address table list in the SNMP engine. This table of transport addresses is used in the generation of SNMP messages.

Table 164. *Target Address Table Configuration Commands*

Command Syntax and Usage
snmp-server target-address *<1-16>* **{address|address6}** *<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|address6}** *<transport IP address>* Configures a transport IPv4/IPv6 address that can be used in the generation of SNMP traps. **Note:** IPv6 addresses are not displayed in the configuration, but they do receive traps. **Command mode:** Global configuration
snmp-server target-address *<1-16>* **parameters-name** *<1-32 characters>* Defines the name as defined in the following command on page 315: `snmp-server target-parameters` *<1-16>* `name` *<1-32 characters>* **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
no snmp-server target-address *<1-16>* Deletes the Target Address Table entry. **Command mode:** Global configuration
show snmp-server v3 target-address *<1-16>* Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

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

Table 165. *Target Parameters Table Configuration Commands*

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
`snmp-server target-parameters` *<1-16>* **`message {snmpv1|snmpv2c|snmpv3}`** Allows you to configure the message processing model that is used to generate SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters` *<1-16>* **`name`** *<1-32 characters>* Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry. **Command mode:** Global configuration
`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 309) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration

Table 165. *Target Parameters Table Configuration Commands (continued)*

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

SNMPv3 Notify Table Configuration

SNMPv3 uses Notification Originator to send out traps. A notification typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.

Table 166. *Notify Table 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 167. *System Access Configuration Commands*

Command Syntax and Usage
[no] access http enable Enables or disables HTTP (Web) access to the Browser-Based Interface. The default settings is `disabled`. **Command mode:** Global configuration
[default] access http port [<*port number*>**]** Sets the switch port used for serving switch Web content. The default setting is `HTTP port 80`. **Command mode:** Global configuration
[no] access snmp {read-only|read-write} Enables or disables read-only/write-read SNMP access. **Command mode:** Global configuration
[no] access telnet enable Enables or disables Telnet access. The default settings 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

Table 167. *System Access Configuration Commands (continued)*

Command Syntax and Usage
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
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 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
[no] access userbbi enable Enables or disables user configuration access through the Browser-Based Interface (BBI). **Command mode:** Global configuration
show access Displays the current system access parameters. **Command mode:** All

Management Network Configuration

These commands are used to define IP address ranges which are allowed to access the switch for management purposes.

Table 168. *Management Network Configuration Commands*

Command Syntax and Usage
[no] access management-network *<mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length>* Adds or removes a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Lenovo N/OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a "Network Down" state on the network. **Command mode:** Global configuration
access management-network *<mgmt network IPv4 address> <mgmt network mask>* **{snmp-ro|snmp-rw}** Adds a defined IPv4 network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IP address and mask address in dotted-decimal notation. **Command mode:** Global configuration
no access management-network {snmp-ro|snmp-rw} Clears the IPv4 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
access management-network6 *<mgmt network IPv6 address> <IPv6 prefix length>* **{snmp-ro|snmp-rw}** Adds a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed. **Command mode:** Global configuration
no access management-network6 {snmp-ro|snmp-rw} Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
show access management-network Displays the current management network configuration and SNMP access management IP list. **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 169. *User Access Control Configuration Commands*

Command Syntax and Usage
access user *<1-20>* Configures the User ID. **Command mode:** Global configuration
[no] access user administrator-enable Enables or disables the default administrator account. **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. **Note:** Access includes "oper" functions. **Command mode:** Global configuration
access user operator-password *<1-128 characters>* Sets the operator (oper)password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports. **Command mode:** Global configuration
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 eject {*<user name>***|***<session ID>***}** Ejects the specified user from the CN4093. **Command mode:** Global configuration
clear line *<1-12>* Ejects the user with the corresponding session ID from the CN4093. **Command mode:** All except User EXEC
show access user Displays the current user status. **Command mode:** All

System User ID Configuration

The following table describes user ID configuration commands.

Table 170. *User ID Configuration Commands*

Command Syntax and Usage
[no] access user *<1-20>* **enable** Enables or disables the user ID. **Command mode:** Global configuration
access user *<1-20>* **level {user|operator|administrator}** Sets the Class-of-Service to define the user's authority level. Lenovo N/OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level. **Command mode:** Global configuration
access user *<1-20>* **name** *<1-8 characters>* Defines the user name of maximum eight characters. **Command mode:** Global configuration
access user *<1-20>* **password** Sets the user (user) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Command mode:** Global configuration
no access user *<1-20>* Deletes the user ID. **Command mode:** Global configuration
show access user Displays the current user ID configuration. **Command mode:** All

Strong Password Configuration

The following table describes strong password configuration commands.

Table 171. *Strong Password Configuration Commands*

Command Syntax and Usage
[no] access user strong-password enable Enables or disables Strong Password requirement. **Command mode:** Global configuration
access user strong-password clear local user {lockout|fail-attempts} {<*username*>**|all}** Enables locked out accounts or resets failed login counters for all users or for a specific user. **Command mode:** Global configuration
access user strong-password expiry <*1-365*> Configures the number of days allowed before the password must be changed. The default value is `60`. **Command mode:** Global configuration
access user strong-password faillock <*1-10*> Configures the number of failed login attempts that trigger the account lockout. The default value is `6`. **Command mode:** Global configuration
access user strong-password faillog <*1-255*> Configures the number of failed login attempts allowed before a security notification is logged. The default value is `3`. **Command mode:** Global configuration
[no] access user strong-password lockout Enables or disables account lockout after a specified number of failed login attempts. The default setting is `disabled`. **Command mode:** Global configuration

Table 171. *Strong Password Configuration Commands*

Command Syntax and Usage
access user strong-password warning *<1-365>* Configures the number of days before password expiration, that a warning is issued to users. The default value is 15. **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 172. *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
access https generate-certificate Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: o Country Name (2 letter code): CA o State or Province Name (full name): Ontario o Locality Name (for example, city): Ottawa o Organization Name (for example, company): Lenovo o Organizational Unit Name (for example, section): Operations o Common Name (for example, user's name): Mr Smith o Email (for example, email address): info@lenovo.com You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent. **Command mode:** Global configuration

Table 172. *HTTPS Access Configuration Commands*

Command Syntax and Usage
[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 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 173. *Custom DST Configuration Commands*

Command Syntax and Usage
[no] system custom-dst enable Enables or disables the Custom Daylight Saving Time settings. **Command mode:** Global configuration
system custom-dst start-rule <*WDDMMhh*> Configures the start date for custom DST, as follows: WDMMhh W = week (0-5, where 0 means use the 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
show custom-dst Displays the current Custom DST configuration. **Command mode:** All

sFlow Configuration

Lenovo N/OS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use these commands to configure the sFlow agent on the switch.

Table 174. *sFlow Configuration Commands*

Command Syntax and Usage
`[no] sflow enable` Enables or disables the sFlow agent. **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
`sflow server` *<IP address>* Defines the sFlow server address. **Command mode:** Global configuration
`show sflow` Displays sFlow configuration parameters. **Command mode:** All

sFlow Port Configuration

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

Table 175. *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), see "Management Port Configuration" on page 339.

Table 176. *Port Configuration Commands*

Command Syntax and Usage
`interface port` *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
`[no] bpdu-guard` Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled. **Command mode:** Interface port
`description` *<1-64 characters>* Sets a description for the port. The assigned port name appears next to the port description on some information and statistics screens. The default is set to the port number. **Command mode:** Interface port
`dot1p` *<0-7>* Configures the port's 802.1p priority level. **Command mode:** Interface port
`[no] dscp-marking` Enables or disables DSCP re-marking on a port. **Command mode:** Interface port
`[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
`[no] learning` Enables or disables FDB learning on 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

Table 176. *Port Configuration Commands (continued)*

Command Syntax and Usage
`[no] reflective-relay force` Enables or disables constraint to always keep reflective relay active. The default setting is `disabled`. **Command mode:** Interface port
`[no] rmon` Enables or disables Remote Monitoring for the port. RMON must be `enabled` for any RMON configurations to function. **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 333.) **Command mode:** Interface port
`no shutdown` Enables the port. **Command mode:** Interface port
`[no] storm-control broadcast level rate` *<0-2097151>* 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] storm-control multicast level rate` *<0-2097151>* 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] storm-control unicast level rate` *<0-2097151>* 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

Table 176. *Port Configuration Commands (continued)*

Command Syntax and Usage
`switchport mode {access|trunk|private-vlan}` Configures the port's trunking mode: o `access` allows association to a single VLAN o `trunk` automatically adds the port to all created VLANs. To configure a specific allowed VLAN range for the port use the command: `switchport trunk allowed vlan` o `private-vlan` allows association to a private VLAN The default mode is `access`. **Note**: When switching from access to trunk mode, the port inherits the access VLAN as the trunk Native-VLAN. **Note**: When switching from trunk to access mode, the port inherits the trunk Native-VLAN as the access VLAN. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan` *<VLAN ID range>* Configures the allowed VLANs in trunk mode for the current port or portchannel. If the allowed range does not have any existing VLANs, the lowest-numbered VLAN is created and becomes the Native-VLAN. If the allowed range contains an existing VLAN(s), but the Native-VLAN is not in the allowed range, the Native-VLAN is changed to the lowest-numbered existing VLAN. If a new VLAN is created and it is part of the allowed VLAN range, the port will also be added to that VLAN. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {add|remove}` *<VLAN ID range>* Updates the associated VLANs in trunk mode. o `add` enables the VLAN range in addition to the current configuration. If any VLAN in the range does not exist, it will not be created and enabled automatically. o `remove` eliminates the VLAN range from the current configuration. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {all|none}` Updates the associated VLANs in trunk mode. o `all` associates the port to all existing regular VLANs and to any other VLAN that gets created afterwards. o `none` removes the port from all currently associated VLANs and assigns the port to the default Native-VLAN (`VLAN 1` for data ports). **Command mode:** Interface port/Interface portchannel
`no switchport trunk allowed vlan` Assigns the port to all available data VLANs. **Command mode:** Interface port/Interface portchannel

Table 176. *Port Configuration Commands (continued)*

Command Syntax and Usage
`switchport trunk native vlan` *<1-4094>* Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is `1` for data ports and `4095` for the management port. **Command mode:** Interface port/Interface portchannel
`switchport access vlan` *<1-4094>* Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is `1` for data ports and `4095` for the management port. **Command mode:** Interface port/Interface portchannel
`no switchport access vlan` Resets the access VLAN to its default value. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan mapping` *<primary VLAN>* Enables or disables a private VLAN promiscuous port to/from a primary VLAN. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan host-association` *<primary VLAN> <secondary VLAN>* Adds or removes a private VLAN host port to/from a secondary VLAN. **Command mode:** Interface port/Interface portchannel
`[no] tagpvid-ingress` Enables or disables tagging the ingress frames with the port's VLAN ID. When `enabled`, the PVID tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID. The default setting is `disabled`. **Command mode**: Interface port/Interface portchannel
`unicast-bandwidth` *<10-100>* Configures the allocated bandwidth percentage for unicast traffic on the port. The remaining bandwidth is automatically allocated to multicast traffic. The default value is `50`. **Command mode:** Interface port

Table 176. *Port Configuration Commands (continued)*

Command Syntax and Usage
`unicast-bandwidth global` *<10-100>* Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is `50`. **Note:** This applies to all ports. **Command mode:** Interface port
`[no] vlan dot1q tag native` Enables or disables VLAN tag persistence. When `disabled`, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is `disabled`. **Note:** In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterward. Also, as an operational command, it will not be dumped into the configuration file. **Command mode:** Global configuration/Interface port/Interface portchannel
`show interface port` *<port alias or number>* Displays 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 177. *Port Error Disable Commands*

Command Syntax and Usage
`[no] errdisable link-flap enable` Enables or disables Link Flap Dampening on the port. For more information, see "Link Flap Dampening Configuration" on page 288. **Command mode:** Interface port
`[no] errdisable recovery` Enables or disables automatic error-recovery for the port. The default setting is `enabled`. **Note**: Error-recovery must be `enabled` globally before port-level commands become active. **Command mode:** Interface port
`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 178. *Port Link Configuration Commands*

Command Syntax and Usage
`[no] auto` Enables or disables auto-negotiation on the port. **Command mode:** Interface port
`duplex {full|half|auto}` Sets the operating mode. The choices include: – Auto negotiation (default) – Half-duplex – Full-duplex **Command mode:** Interface port
`flowcontrol {receive|send} {on|off}` Enables or disables flow control receive or transmit. **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
`speed {`*1000*`|`*10000*`|auto}`** Sets the link speed. Some options are not valid on all ports. The choices include: – 1000 Mbps – 10000 Mbps – any (auto negotiate port speed) **Command mode:** Interface port
`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:

```
CN 4093# 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 553 for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 179. *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: o **Normal**: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the "`no`" form to select normal operation. o **Aggressive**: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. **Command mode:** Interface port
`show interface port` *<port 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 180. *Port OAM Configuration Commands*

Command Syntax and Usage
oam [passive] Configures the OAM discovery mode, as follows: o **Passive**: This port allows its peer link to initiate OAM discovery. If OAM determines that the port is in an anomalous condition, the port is disabled. **Command mode:** Interface port
no oam [passive] Disables OAM discovery on the port. **Command mode:** Interface port
show interface port *<port number>* **oam** Displays current port OAM parameters. **Command mode:** All

Port ACL Configuration

The following table describes port ACL configuration commands.

Table 181. *Port ACL/QoS Configuration Commands*

Command Syntax and Usage
[no] access-control group *<1-256>* Adds or removes the specified ACL group. You can add multiple ACL groups to a port. **Command mode:** Interface port
[no] access-control list *<1-256>* Adds or removes the specified ACL. You can add multiple ACLs to a port. **Command mode:** Interface port
[no] access-control list6 *<1-128>* Adds or removes the specified IPv6 ACL. You can add multiple ACLs 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 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 346.

Table 182. *Port WRED Options*

Command Syntax and Usage
`[no] random-detect ecn enable` Enables or disables Explicit Congestion Notification (ECN). When ECN is `enabled`, 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
`[no] random-detect enable` Enables or disables 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 183. *Port WRED Transmit Queue Options*

Command Syntax and Usage
[no] random-detect transmit-queue *<0-7>* **enable** Sets the WRED transmit queue configuration to `on` or `off`. **Command mode:** Interface port
[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. **Note:** 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. **Note:** Use the `no` form to clear the WRED threshold value. **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 184. *Management Port Configuration Commands*

Command Syntax and Usage
`[no] auto` Enables or disables auto-negotiation on the port. **Command mode:** Interface port
`duplex {full|half|auto}` Sets the operating mode. The choices include: – Full-duplex – Half-duplex – Auto — for auto negotiation (default) **Command mode:** Interface port
`flowcontrol {receive|send} {on|off}` Activates or deactivates one type of flow control. The choices include: – Receive flow control – Transmit flow control **Command mode:** Interface port
`shutdown` Disables the port. **Command mode:** Interface port
`no shutdown` Enables the port. **Command mode:** Interface port
`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
`show interface port` *<port alias or number>* Displays current port parameters. **Command mode:** All

Stacking Configuration

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. The Stacking Configuration menu is used to configure a stack, and to define the Backup switch.

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see "Stacking Boot Options" on page 568.

Table 185. *Stacking Commands*

Command Syntax and Usage
`[no] stack backup` *<csnum (1-8)>* Defines the backup switch in the stack, based on its configured switch number (csnum). **Command mode:** Global configuration
`[no] stack name` *<1-63 characters>* Defines a name for the stack. **Command mode:** Global configuration
`show stack switch-number` *<csnum (1-8)>* Displays UUID and slot ID for all the configured switches from the stack. **Command mode:** All

Stacking Switch Configuration

The following table describes stacking switch configuration commands.

Table 186. *Stacking Switch Commands*

Command Syntax and Usage
stack switch-number *<csnum (1-8)>* **bay** *<1-4>* Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides. **Command mode:** Global configuration
stack switch-number *<csnum (1-8)>* **bind** *<asnum (1-16)>* Binds the selected switch to the stack, based on its attached switch number (asnum). **Command mode:** Global configuration
stack switch-number *<csnum (1-8)>* **description** *<1-63 characters>* Defines a description for each configured switch number of the stack. **Command mode:** Global configuration
stack switch-number *<csnum (1-8)>* **universal-unic-id** *<UUID>* Binds the selected switch to the stack, based on the UUID of the chassis in which the switch resides. You also must enter the bay number to specify a switch within the chassis. Following is an example UUID: `uuid 49407441b1a511d7b95df58f4b6f99fe` **Command mode:** Global configuration
no stack switch-number *<csnum (1-8)>* Deletes the selected switch from the stack. **Command mode:** Global configuration

Management Interface Configuration

To provide continuous Management IP reachability in the event of a Master node failover, an additional floating Management IP address can be set up on the management IP interface. The floating Management IP address will be used by the backup switch when taking over management from the failed master node.

To configure the floating Management IP address, use the following commands:

Table 187. *Management Interface Options*

Command Syntax and Usage
floating ip address *<IP address>* **[***<IP netmask>***]** Configures the specified IPv4 address as a floating Management IP address. **Command mode:** Interface IP
floating ip netmask *<IP netmask>* Configures the floating IP subnet mask address. **Command mode:** Global configuration
no floating Removes all floating IP addresses. **Command mode:** Interface IP
show interface ip Displays current IP address floating information. **Command mode:** Global configuration

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 188. *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
qos unicast-bandwith *<10-100>* Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is **50**. **Note:** This applies to all ports. **Command mode:** All
show qos transmit-queue Displays the current 802.1p parameters. **Command mode:** All

DSCP Configuration

These commands map the DiffServ Code Point (DSCP) value of incoming packets to a new value or to an 802.1p priority value.

Table 189. *DSCP Configuration Commands*

Command Syntax and Usage
qos dscp dot1p-mapping *<DSCP (0-63)> <priority (0-7)>* Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value. **Command mode:** Global configuration
qos dscp dscp-mapping *<DSCP (0-63)> <new DSCP (0-63)>* Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value. **Command mode:** Global configuration
[no] qos dscp re-marking Enables or disables DSCP re-marking globally. **Command mode:** Global configuration
show qos dscp Displays the current DSCP parameters. **Command mode:** All

Control Plane Protection

To prevent switch instability if the switch is unable to process a high rate of control-plane traffic, the switch now supports CoPP. CoPP, allows you to assign control-plane traffic protocols to one of 48 queues, and can set bandwidth limits for each queue.

Table 190. *CoPP Commands*

Command Syntax and Usage
qos protocol-packet-control packet-queue-map *<packet queue number (0-47)> <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) – **ecp** (ECP packets) – **fips** (FIPS packets) – **icmp** (ICMP packets) – **icmp6** (ICMPv6 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
no qos protocol-packet-control packet-queue-map *<packet type>* Clears the selected packet type from its associated packet queue. **Command mode:** Global configuration

Table 190. *CoPP Commands*

Command Syntax and Usage
qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-47)> <1-10000>* Configures the number of packets per second allowed for each packet queue. **Command mode:** Global configuration
no qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-47)>* 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 337.

Table 191. *WRED Configuration Options*

Command Syntax and Usage
[no] qos random-detect ecn Enables or disables Explicit Congestion Notification (ECN). When ECN is `enabled`, 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

Table 191. *WRED Configuration Options*

Command Syntax and Usage
`[no] qos random-detect enable` Enables or disables Random Detection and avoidance. **Command mode:** Global configuration
`show qos random-detect` Displays current Random Detection and avoidance parameters. **Command mode:** All

WRED Transmit Queue Configuration

The following table displays WRED Transmit Queue configuration commands.

Table 192. *WRED Transmit Queue Options*

Command Syntax and Usage
[no] qos random-detect transmit-queue *<0-7>* **enable** Sets the WRED transmit queue configuration to `on` or `off`. **Command mode:** Global configuration
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. **Command mode:** Global configuration
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. **Command mode:** Global configuration
no qos random-detect transmit-queue *<0-7>* **{tcp|non-tcp}** Clears the specified WRED threshold value. **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 336.

Table 193. *General ACL Configuration Commands*

Command Syntax and Usage
`[no] access-control group` *<1-256>* Configures an ACL Group. To view command options, see page 366. **Command mode:** Global configuration
`[no] access-control list` *<1-256>* Configures an Access Control List. To view command options, see page 350. **Command mode:** Global configuration
`[no] access-control list6` *<1-128>* Configures an Access Control List. To view command options, see page 355. **Command mode:** Global configuration
`show access-control` Displays the current ACL parameters. **Command mode:** All

Access Control List Configuration

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

Table 194. *ACL Configuration Commands*

Command Syntax and Usage
access-control list *<1-256>* **action {permit|deny| |set-priority** *<0-7>***}** Configures a filter action for packets that match the ACL definitions. You can choose to `permit` (pass) or `deny` (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
[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
[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 355. **Command mode:** Global configuration

Ethernet Filtering Configuration

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

Table 195. *Ethernet Filtering Configuration Commands*

Command Syntax and Usage
[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 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 ethernet-type {any|arp|ip|ipv6|mpls|rarp|***<other (0x600-0xFFFF)>***}** Defines the Ethernet type 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 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 196. *IP version 4 Filtering Configuration Commands*

Command Syntax and Usage
[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 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 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 197. *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 `source-port` 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 198. *Packet Format Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control list *<1-256>* **packet-format ethernet {ethertype2|llc|snap}** Defines the Ethernet 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
[no] access-control list *<1-256>* **packet-format tagging {any|none|tagged}** Defines the tagging 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 199. *IPv6 ACL Options*

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

IPv6 Filtering Configuration

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

Table 200. *IP version 6 Filtering Options*

Command Syntax and Usage
[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 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 flow-label** *<0-1048575>* Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **ipv6 next-header** *<0-255>* Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **ipv6 traffic-class** *<0-255>* Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL. **Command mode:** Global configuration
default access-control list6 *<1-128>* **ipv6** Resets the IPv6 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list6 *<1-128>* **ipv6** Displays the current IPv6 parameters. **Command mode:** All

IPv6 TCP/UDP Filtering Configuration

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

Table 201. *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 `source-port` 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 Metering Configuration

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

Table 202. *IPv6 Metering Options*

Command Syntax and Usage
access-control list6 *<1-128>* **meter action {drop|pass}** Configures the ACL Meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control list6 *<1-128>* **meter committed-rate** *<64-40000000>* Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* **meter enable** Enables or disables ACL Metering. **Command mode:** Global configuration
access-control list6 *<1-128>* **meter maximum-burst-size** *<32-4096>* Configures the maximum burst size, in kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode:** Global configuration
default access-control list6 *<1-128>* **meter** Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
no access-control list6 *<1-128>* **meter** Deletes the selected ACL meter. **Command mode:** Global configuration
show access-control list6 *<1-128>* **meter** Displays current ACL Metering parameters. **Command mode:** All

Management ACL Filtering Configuration

These commands allow you to define matching criteria for a Management ACL.

Table 203. *Management ACL Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control macl *<1-128>* **ipv4** Enables or disables the Management ACL. **Command mode:** Global configuration
[no] access-control macl *<1-128>* **ipv4** *<destination IP address>* **[***<address mask>***]** Sets IPv4 filtering to filter on the destination IP address. **Command mode:** Global configuration
[no] access-control macl *<1-128>* **ipv4** *<source IP address>* **[***<address mask>***]** Sets IPv4 filtering to filter on the source IP address. **Command mode:** Global configuration
[no] access-control macl *<1-128>* **ipv4 protocol** *<0-255>* Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed here 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
default access-control list *<1-128>* **ipv4** Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-128>* **packet-format** Displays the current Packet Format parameters for the ACL. **Command mode:** All

TCP/UDP Filtering Configuration

The following commands allow you to define TCP/UDP matching criteria for a Management ACL.

Table 204. *Management ACL TCP/UDP Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control macl *<1-128>* **tcp-udp source-port** *<1-65535>* **[***<mask (0x0-0x3f)>***]** Defines a source port for the Management ACL. If defined, traffic with the specified TCP or UDP source port will match this Management 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 macl *<1-128>* **tcp-udp destination-port** *<1-65535>* **[***<mask (0xFFFF)>***]** Defines a destination port for the Management ACL. If defined, traffic with the specified TCP or UDP destination port will match this Management ACL. Specify the port number, just as with `source-port`. **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

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 350.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration" on page 417.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 534.

Table 205 lists the general VMAP configuration commands.

Table 205. *VMAP Configuration Commands*

Command Syntax and Usage
access-control vmap *<1-128>* **action {permit|deny| |set-priority** *<0-7>***}** Configures a filter action for packets that match the VMAP definitions. You can choose to `permit` (pass) or `deny` (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **egress-port** *<port alias or number>* Configures the VMAP to function on egress packets. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ethernet destination-mac-address** *<MAC address> <MAC mask>* Enables or disables filtering of VMAP statistics collection based on destination MAC. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ethernet source-mac-address** *<MAC address> <MAC mask>* Enables or disables filtering of VMAP statistics collection based on source MAC. **Command mode:** Global configuration

Table 205. *VMAP Configuration Commands (continued)*

Command Syntax and Usage
[no] access-control vmap *<1-128>* **ethernet ethernet-type {***<0x600-0xFFF>***|any|arp|rarp|ip|ipv6|mpls}** Enables or disables filtering of VMAP statistics collection based on the encapsulated protocol: o **<0x600-0xFFF>** filters Ethernet frames with the specified EtherType o **any** filters all frames o **arp** filters Address Resolution Protocol frames o **rarp** filters Reverse Address Resolution Protocol frames o **ip** filters Internet Protocol version 4 frames o **ipv6** filters Internet Protocol version 6 frames o **mpls** filters Multiprotocol Label Switching frames **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ethernet priority** *<0-7>* Enables or disables filtering of VMAP statistics collection based on the IEEE 802.1Q priority code point value. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ethernet vlan** *<1-4094>* Enables or disables filtering of VMAP statistics collection based on VLAN ID. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ipv4 destination-ip-address** *<IPv4 address> <IPv4 mask>* Enables or disables filtering of VMAP statistics collection based on destination IP address. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ipv4 source-ip-address** *<IPv4 address> <IPv4 mask>* Enables or disables filtering of VMAP statistics collection based on source IP address. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ipv4 protocol** *<0-255>* Enables or disables filtering of VMAP statistics collection based on protocol. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **ipv4 type-of-service** *<0-255>* Enables or disables filtering of VMAP statistics collection based on type of service. **Command mode:** Global configuration

Table 205. *VMAP Configuration Commands (continued)*

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

Table 205. *VMAP Configuration Commands (continued)*

Command Syntax and Usage
access-control vmap *<1-128>* **packet-format tagging {any|none|tagged}** Sets filtering based on packet tagging. The options are: – `any`: Filter tagged & untagged packets – `none`: Filter only untagged packets – `tagged`: Filter only tagged packets **Command mode:** Global configuration
no access-control vmap *<1-128>* **packet-format {ethernet|ip|tagging}** Disables filtering based on the specified packet format. **Command mode:** Global configuration
access-control vmap *<1-128>* **re-mark dot1p** *<0-7>* Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark dot1p** Disables the use of dot1p for in-profile traffic ACL re-mark configuration. **Command mode:** Global configuration
access-control vmap *<1-128>* **re-mark {in-profile|out-profile} dscp** *<0-63>* Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
no access-control vmap *<1-128>* **re-mark {in-profile| |out-profile}** Removes all re-mark in-profile or out-profile settings. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **re-mark use-tos-precedence** Enables or disables the use of the TOS precedence for in-profile traffic. **Command mode:** Global configuration
[no] access-control vmap *<1-128>* **statistics** Enables or disables the statistics collection for the VMAP. **Command mode:** Global configuration
access-control vmap *<1-128>* **tcp-udp {source-port| |destination-port}** *<1-65535>* **[***<port mask (0x0001 - 0xFFFF)>***]** Sets the TCP/UDP filtering source port or destination port and port mask for this ACL. **Command mode:** Global configuration

Table 205. *VMAP Configuration Commands (continued)*

Command Syntax and Usage
access-control vmap *<1-128>* **tcp-udp flags** *<value (0x0-0x3F)>* **[***<flags mask (0x0-0x3F)>***]** Sets the TCP flags for this ACL. **Command mode:** Global configuration
no access-control vmap *<1-128>* **tcp-udp** Removes TCP/UDP filtering for this ACL. **Command mode:** Global configuration
default access-control vmap *<1-128>* Resets the VMAP parameters to their default values. **Command mode:** Global configuration
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 206. *ACL Group Configuration Commands*

Command Syntax and Usage
[no] access-control group *<1-256>* **list** *<1-256>* Adds or removes the selected ACL to/from the ACL group. **Command mode:** Global configuration
[no] access-control group *<1-256>* **list6** *<1-128>* Adds or removes the selected IPv6 ACL to/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 207. *ACL Metering Configuration Commands*

Command Syntax and Usage
access-control list *<1-256>* **meter action {drop|pass}** Configures the ACL meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control list *<1-256>* **meter committed-rate** *<64-10000000>* Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
[no] access-control list *<1-256>* **meter enable** Enables or disables ACL Metering. **Command mode:** Global configuration
access-control list *<1-256>* **meter maximum-burst-size** *<32-4096>* Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode:** Global configuration
default access-control list *<1-256>* **meter** Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
no access-control list *<1-256>* **meter** 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. 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 208. *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

The following table displays Re-marking In-profile configuration commands.

Table 209. *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
no access-control list *<1-256>* **re-mark in-profile** Removes all re-mark in-profile settings. **Command mode:** Global configuration
show access-control list *<1-256>* **re-mark** Displays current re-mark parameters. **Command mode:** All

Re-Marking Out-Profile Configuration

The following table displays Re-marking Out-profile configuration commands.

Table 210. *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** Removes all re-mark out-profile settings. **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 IPv6 header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within or outside the ACL metering profile.

Table 211. *IPv6 General Re-Mark Options*

Command Syntax and Usage
access-control list6 *<1-128>* **re-mark dot1p** *<0-7>* Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark dot1p** Disables use of 802.1p value for re-marked packets. **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

The following table displays IPv6 Re-marking In-profile configuration commands.

Table 212. *IPv6 Re-Mark In-Profile Options*

Command Syntax and Usage
access-control list6 *<1-128>* **re-mark in-profile dscp** *<0-63>* Re-marks the DSCP value for in-profile traffic. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark in-profile dscp** Disables the use of DSCP for the in-profile traffic. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark in-profile** Removes all re-mark in-profile settings. **Command mode:** Global configuration
show access-control list6 *<1-128>* **re-mark** Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking Out-Profile Configuration

The following table displays IPv6 Re-marking Out-profile configuration commands.

Table 213. *IPv6 Re-Mark Out-of-Profile Options*

Command Syntax and Usage
access-control list6 *<1-128>* **re-mark out-profile dscp** *<0-63>* Re-marks the DSCP value on out-of-profile packets for the ACL. **Command mode:** Global configuration
no access-control list6 *<1-128>* **re-mark out-profile** Removes all re-marking out-of-profile settings. **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 *Lenovo N/OS 8.2 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 214. *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

The following table displays Port Mirror configuration commands.

Table 215. *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. **Note:** Up to two monitor ports with 2-way mirroring or four monitor ports with 1-way mirroring are supported in stand-alone mode. In stacking mode, the switch supports one monitor port with 2-way mirroring or two monitor ports with 1-way mirroring. **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 216. *Layer 2 Configuration Commands*

Command Syntax and Usage
spanning-tree mode disable 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
vlan *<VLAN number>* Enter VLAN configuration mode. To view command options, see page 417. **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 217. *802.1X Configuration Commands*

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

802.1X Global Configuration

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

Table 218. *802.1X Global Configuration Commands*

Command Syntax and Usage
`dot1x max-request` *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is `2`. **Command mode:** Global configuration
`dot1x mode [force-unauthorized|auto|force-authorized]` Sets the type of access control for all ports: o `force-unauthorized` - the port is unauthorized unconditionally. o `auto` - the port is unauthorized until it is successfully authorized by the RADIUS server. o `force-authorized` - the port is authorized unconditionally, allowing all traffic. The default value is `force-authorized`. **Command mode:** Global configuration
`dot1x quiet-time` *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is `60`. **Command mode:** Global configuration

Table 218. *802.1X Global Configuration Commands (continued)*

Command Syntax and Usage
`[no] dot1x re-authenticate` Sets the re-authentication status to `on` or `off`. The default value is `off`. **Command mode:** Global configuration
`dot1x re-authentication-interval` *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is `3600`. **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`. 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`). **Command mode:** Global configuration
`dot1x supplicant-timeout` *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet from the authentication server. The default value is `30`. **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`. **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

Table 218. *802.1X Global Configuration Commands (continued)*

Command Syntax and Usage
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 219. *802.1X Guest VLAN Configuration Commands*

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

802.1X Port Configuration

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

Table 220. *802.1X Port Commands*

Command Syntax and Usage
dot1x apply-global Applies current global 802.1X configuration parameters to the port. **Command mode:** Interface port
dot1x max-request *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2. **Command mode:** Interface port
dot1x mode {force-unauthorized|auto|force-authorized} Sets the type of access control for the port: o `force-unauthorized` - the port is unauthorized unconditionally. o `auto` - the port is unauthorized until it is successfully authorized by the RADIUS server. o `force-authorized` - the port is authorized unconditionally, allowing all traffic. The default value is `force-authorized`. **Command mode:** 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`. **Command mode:** Interface port
[no] dot1x re-authenticate Sets the re-authentication status to `on` or `off`. The default value is `off`. **Command mode:** Interface port
dot1x re-authentication-interval *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is `3600`. **Command mode:** Interface port

Table 220. *802.1X Port Commands (continued)*

Command Syntax and Usage
dot1x server-timeout *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is `30`. 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 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`. **Command mode:** Interface port
dot1x transmit-interval *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is `30`. **Command mode:** Interface port
[no] dot1x vlan-assign Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`. **Command mode:** Interface port
default dot1x Resets the 802.1X port parameters to their default values. **Command mode:** Interface port
show interface port *<port alias or number>* **dot1x** Displays current 802.1X port parameters. **Command mode:** All

Spanning Tree Configuration

Lenovo Networking OS supports the IEEE 802.1D (2004) Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1Q (2003) Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST+). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

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

Table 221. *Spanning Tree Configuration Options*

Command Syntax and Usage
spanning-tree mode [disable|mst|pvrst|rstp] Selects and enables Multiple Spanning Tree mode (mst), Per VLAN Rapid Spanning Tree mode (pvrst), or Rapid Spanning Tree mode (rstp). The default mode is PVRST+. When you select **spanning-tree mode disable**, the switch globally turns Spanning Tree off. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command. **Command mode:** Global configuration
[no] spanning-tree pvst-compatibility Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is enabled. **Command mode:** Global configuration
[no] spanning-tree stg-auto Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool. **Note**: When using VASA, a maximum number of 128 automatically assigned STGs is supported. **Note**: VASA applies only to PVRST mode. **Command mode:** Global configuration
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 221. *Spanning Tree Configuration Options (continued)*

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
[no] spanning-tree link-type {p2p|shared|auto} Defines the type of link connected to the port, as follows: – `auto`: Configures the port to detect the link type, and automatically match its settings. – `p2p`: Configures the port for Point-To-Point protocol. – `shared`: Configures the port to connect to a shared medium (usually a hub). The default link type is `auto`. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree portfast Enables or disables this port as portfast or edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (`enabled`). **Note**: After you configure the port as an edge port, you must disable the port and then re-enable the port for the change to take effect. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree pvst-protection Enables or disables PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it is `error disabled`. The default setting for this feature is `disabled` (no protection). **Command mode:** Interface port/Interface portchannel

Table 221. *Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
show spanning-tree Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (RSTP, PVRST, or MSTP), and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: – 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 For details, see page 74. **Command mode:** All
show spanning-tree blockedports Lists the ports blocked by each STP instance. **Command mode:** All
show spanning-tree root Displays the Spanning Tree configuration on the root bridge for each STP instance. For details, see page 82. **Command mode:** All
show spanning-tree [vlan *<VLAN ID>***] bridge** Displays Spanning Tree bridge information. For details, see page 81. **Command mode:** All

MSTP Configuration

Up to 32 Spanning Tree Groups can be configured in MSTP mode. MSTP is turned off by default and the default STP mode is PVRST+.

Note: When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 128.

Table 222. *Multiple Spanning Tree Configuration Options*

Command Syntax and Usage
`[no] spanning-tree mst` *<0-32>* **`enable`** Enables or disables the specified MSTP instance. **Command mode:** Global configuration
`spanning-tree mst forward-time` *<4-30>* Configures the forward delay time in seconds. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The default value is `15`. **Command mode:** Global configuration
`spanning-tree mst max-age` *<6-40>* Configures the maximum age interval in seconds. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The default value is `20`. **Command mode:** Global configuration
`spanning-tree mst` *<0-32>* **`priority`** *<0-65535>* Configures the CIST bridge priority for the specified MSTP instance. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...). The default value is `61440`. **Command mode:** Global configuration
`spanning-tree mst max-hops` *<4-60>* Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default value is `20`. **Command mode:** Global configuration

Table 222. *Multiple Spanning Tree Configuration Options (continued)*

Command Syntax and Usage
default spanning-tree mst *<0-32>* Restores the Spanning Tree instance to its default configuration. **Command mode:** Global configuration
no spanning-tree mst configuration Returns the MST region to its default values: no VLAN is mapped to any MST instance. Revision number is reset to **0**. **Command mode**: Global configuration
spanning-tree mst configuration Enables MSTP configuration mode. **Command mode**: Global configuration
[no] instance *<0-32>* **vlan** *<VLAN numbers>* Maps or removes the specified VLANs to the Spanning Tree instance. If a VLAN does not exist, it will not be created automatically. **Command mode:** MST configuration
[no] name *<1-32 characters>* Configures a name for the MSTP region. All devices within an MSTP region must have the same region name. **Command mode:** MST configuration
[no] revision *<0-65535>* Configures a revision number for the MSTP region. The revision is used as a numerical identifier for the region. All devices within an MSTP region must have the same revision number. **Command mode:** MST configuration
show spanning-tree mst *<0-32>* **[information]** Displays the current MSTP configuration for the specified instance. **Command mode:** All
show spanning-tree mst configuration Displays the current MSTP settings. **Command mode:** All

MSTP Port Configuration

MSTP port parameters are used to modify MSTP operation on an individual port basis. MSTP parameters do not affect operation of RSTP/PVRST.

Table 223. *MSTP Port Configuration Options*

Command Syntax and Usage
spanning-tree mst *<0-32>* **cost** *<0-200000000>* Configures the port path cost for the specified MSTP instance. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: o 1Gbps = 20000 o 10Gbps = 2000 The default value of `0` indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port/Interface portchannel
[no] spanning-tree mst *<0-32>* **enable** Enables or disables the specified MSTP instance on the port. **Command mode:** Interface port/Interface portchannel
spanning-tree mst hello-time *<1-10>* Configures the 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. The default value is `2`. **Command mode:** Interface port/Interface portchannel
spanning-tree mst *<0-32>* **port-priority** *<0-240>* Configures the port priority for the specified MSTP instance. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...). The default value is `128`. **Command mode:** Interface port/Interface portchannel

Table 223. *MSTP Port Configuration Options (continued)*

Command Syntax and Usage
`[no] spanning-tree pvst-protection` Configures PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is `disabled`. **Note**: Not available in stacking. **Command mode:** Interface port
`show interface port` *<port alias or number>* **`spanning-tree mstp cist`** Displays the current CIST port configuration. **Command mode:** All

RSTP/PVRST Configuration

Table 224 describes the commands used to configure the Rapid Spanning Tree (RSTP) and Per VLAN Rapid Spanning Tree Protocol (PVRST+) protocols.

Table 224. *RSTP/PVRST Configuration Options*

Command Syntax and Usage
`[no] spanning-tree stp` *<STG number>* **`enable`** Enables or disables Spanning Tree instance. The default settings is `enabled`. **Command mode:** Global configuration
`spanning-tree stp` *<STG number>* **`vlan`** *<VLAN number>* Associates a VLAN with a Spanning Tree Group and requires a VLAN ID as a parameter. If the VLAN does not exist, it will be created automatically, but it will be `disabled` by default. **Command mode:** Global configuration
`no spanning-tree stp` *<STG number>* **`vlan`** *<VLAN number>* Breaks the association between a VLAN and a Spanning Tree Group and requires a VLAN ID as a parameter. **Command mode:** Global configuration
`no spanning-tree stp` *<STG number>* **`vlan all`** Removes all VLANs from a Spanning Tree Group. **Command mode:** Global configuration

Table 224. *RSTP/PVRST Configuration Options (continued)*

Command Syntax and Usage
`default spanning-tree stp` *<STG number>* Restores a Spanning Tree instance to its default configuration. **Command mode:** Global configuration
`show spanning-tree stp` *<STG number>* **`[information]`** Displays current Spanning Tree Protocol parameters for the specified Spanning Tree Group. See page 79 for details about the `information` parameter. **Command mode:** All

Bridge RSTP/PVRST Configuration

Spanning Tree bridge parameters affect the global STG operation of the switch. STG bridge parameters include:

- Bridge priority
- Bridge hello time
- Bridge maximum age
- Forwarding delay

Table 225. *Bridge Spanning Tree Configuration Options*

Command Syntax and Usage
`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. The default value is `15`. **Note:** This command does not apply to MSTP. **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. The default value is `2`. **Note:** This command does not apply to MSTP. **Command mode:** Global configuration

Table 225. *Bridge Spanning Tree Configuration Options*

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. The default value is `20`. **Note:** This command does not apply to MSTP. **Command mode:** Global configuration
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 range is 0 to 65535, in steps of 4096 (0, 4096, 8192...). The default value is `61440`. **Command mode:** Global configuration
show spanning-tree [vlan *<VLAN ID>***] bridge** Displays the current Spanning Tree parameters either globally or for a specific VLAN. See page 81 for sample output. **Command mode:** All

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

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

By default, Spanning Tree is turned `off` for management ports, and turned `on` for data ports. STG port parameters include:

- Port priority
- Port path cost

Table 226. *Spanning Tree Port Options*

Command Syntax and Usage
`[no] spanning-tree stp` *<STG number>* **`enable`** Enables or disables STG on the port. **Command mode:** Interface port
`spanning-tree stp link-type {auto|p2p|shared}` Defines the type of link connected to the port, as follows: o `auto`: Configures the port to detect the link type, and automatically match its settings. o `p2p`: Configures the port for Point-To-Point protocol. o `shared`: Configures the port to connect to a shared medium (usually a hub). **Command mode:** Interface port
`spanning-tree stp` *<STG number>* **`path-cost`** *<1-200000000, 0 for default)>* Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: o 1Gbps = 20000 o 10Gbps = 2000 The default value of `0` indicates that the default path cost will be computed for an auto negotiated link speed. **Command mode:** Interface port
`spanning-tree stp` *<STG number>* **`priority`** *<0-240>* Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...). The default value is `128`. **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 227. *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. With MAC Address Notification `enabled`, the switch generates a syslog message when a MAC address is added or removed from the MAC address table. **Note:** This is applicable for internal ports only. **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 228. *Static Multicast MAC Configuration Commands*

Command Syntax and Usage
`[no] mac-address-table multicast` *<MAC address> <VLAN number> <port alias or number>* Adds or deletes a permenant multicast FDB 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 all` Deletes all permenant multicast FDB entries. **Command mode:** Global configuration
`mac-address-table multicast reload` Reloads all permenant multicast FDB entries. **Command mode:** Global configuration
`show mac-address-table multicast` Display the current permenant multicast FDB entries. **Command mode**: All

Static FDB Configuration

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

Table 229. *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
show mac-address-table Display current FDB configuration. **Command mode**: All

ECP Configuration

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

Table 230. *ECP Configuration Options*

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

LLDP Configuration

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

Table 231. *LLDP Configuration Commands*

Command Syntax and Usage
`[no] lldp enable` Globally enables or disables LLDP. The default setting is `enabled`. **Command mode**: Global configuration
`lldp holdtime-multiplier` *<2-10>* Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is `4`. **Command mode**: Global configuration
`no lldp holdtime-multiplier` Sets the message hold time multiplier to its default value of `4`. **Command mode:** Global configuration
`lldp refresh-interval` *<5-32768>* Configures the message transmission interval, in seconds. The default value is `30`. **Command mode**: Global configuration
`no lldp refresh-interval` Sets the message transmission interval to its default value of `30` seconds. **Command mode:** Global configuration
`lldp reinit-delay` *<1-10>* Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages. The default value is `2`. **Command mode**: Global configuration
`no lldp reinit-delay` Sets the re-initialization delay interval to its default value of `2` seconds. **Command mode:** Global configuration
`lldp transmission-delay` *<1-8192>* Configures the transmission delay interval, in seconds. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port. The default value is `2`. **Command mode**: Global configuration

Table 231. *LLDP Configuration Commands*

Command Syntax and Usage
no lldp transmission-delay Sets the transmission delay interval to its default value of 2 seconds. **Command mode:** Global configuration
lldp trap-notification-interval *<1-3600>* Configures the trap notification interval, in seconds. The default value is 5. **Command mode**: Global configuration
no lldp trap-notification-interval Sets the trap notification interval to its default value of 5 seconds. **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 232. *LLDP Port Commands*

Command Syntax and Usage
lldp admin-status {tx_only|rx_only|tx_rx} Configures the LLDP transmission type for the port, as follows: o Transmit only o Receive only o Transmit and receive The default setting is tx_rx. **Command mode**: Interface port
no lldp admin-status Disables LLDP transmission for the port. **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 233. *Optional TLV Commands*

Command Syntax and Usage
[no] lldp tlv all Enables or disables all optional TLV information types. **Command mode**: Interface port
[no] lldp tlv dcbx Enables or disables the Data Center Bridging Capability Exchange (DCBX) information type. **Command mode**: Interface port
[no] lldp tlv framesz Enables or disables the Maximum Frame Size information type. **Command mode**: Interface port
[no] lldp tlv linkaggr Enables or disables the Link Aggregation information type. **Command mode**: Interface port
[no] lldp tlv macphy Enables or disables the MAC/Phy Configuration information type. **Command mode**: Interface port
[no] lldp tlv mgmtaddr Enables or disables the Management Address information type. **Command mode**: Interface port
[no] lldp tlv portdesc Enables or disables the Port Description information type. **Command mode**: Interface port
[no] lldp tlv portprot Enables or disables the Port and VLAN Protocol ID information type. **Command mode**: Interface port
[no] lldp tlv portvid Enables or disables the Port VLAN ID information type. **Command mode**: Interface port
[no] lldp tlv powermdi Enables or disables the Power via MDI information type. **Command mode**: Interface port

Table 233. *Optional TLV Commands (continued)*

Command Syntax and Usage
[no] lldp tlv protid Enables or disables the Protocol ID information type. **Command mode**: Interface port
[no] lldp tlv syscap Enables or disables the System Capabilities information type. **Command mode**: Interface port
[no] lldp tlv sysdescr Enables or disables the System Description information type. **Command mode**: Interface port
[no] lldp tlv sysname Enables or disables the System Name information type. **Command mode**: Interface port
[no] lldp tlv vlanname Enables or disables the VLAN Name information type. **Command mode**: Interface port
show interface port *<port alias or number>* **lldp** Display current LLDP port configuration. **Command mode**: All

Trunk Configuration

Trunk groups can provide super-bandwidth connections between CN4093 or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Two trunk types are available: static trunk groups (portchannels) and dynamic LACP trunk groups (portchannels).

The two trunk types can be configured using the following portchannel ranges:

- static portchannels: 1-64
- LACP portchannels: 65-128

Up to 64 static 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-Lenovo devices must comply with Cisco® EtherChannel® technology and exclude the PAgP networking protocol.

By default, each trunk group is empty and disabled.

Table 234. *Trunk Configuration Commands*

Command Syntax and Usage
`portchannel` *<1-64>* **`port`** *<port alias or number>* **`[enable]`** 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 (-). The `enable` option also enables the trunk group. **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
`[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 235 combined with the hash parameters listed in Table 237.

Table 235. *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

FCoE Trunk Hash Configuration

Use the following commands to configure FCoE Trunk Hash parameters for the CN4093.

Table 236. *FCoE Trunk Hash Configuration Commands*

Command Syntax and Usage
[no] portchannel thash fcoe cntag-id Enables or disables FCoE trunk hashing on the cntag id. **Command mode:** Global configuration
[no] portchannel thash fcoe destination-id Enables or disables FCoE trunk hashing on the destination id. **Command mode:** Global configuration
[no] portchannel thash fcoe fabric-id Enables or disables FCoE trunk hashing on the fabric id. **Command mode:** Global configuration
[no] portchannel thash fcoe originator-id Enables or disables FCoE trunk hashing on the originator id. **Command mode:** Global configuration
[no] portchannel thash fcoe responder-id Enables or disables FCoE trunk hashing on the responder id. **Command mode:** Global configuration
[no] portchannel thash fcoe source-id Enables or disables FCoE trunk hashing on the source id. **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 237. *Layer 2 Trunk Hash Options*

Command Syntax and Usage
[no] portchannel thash l2hash l2-destination-mac-address Enables or disables Layer 2 trunk hashing on the destination MAC. **Command mode:** Global configuration
[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-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 238. *Layer 3 Trunk Hash Options*

Command Syntax and Usage
`[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-ip-address` Enables or disables Layer 3 trunk hashing on the source 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
`[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
`show portchannel hash` Displays the current trunk hash settings. **Command mode:** All

Virtual Link Aggregation Control Protocol Configuration

Use the following commands to configure Virtual Link Aggregation Control Protocol (vLAG) for the CN4093.

Table 239. *Virtual Link Aggregation Control Protocol Commands*

Command Syntax and Usage
[no] vlag enable Enables or disables vLAG globally. **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
vlag auto-recovery *<240-3600>* Sets the duration in seconds of the auto-recovery timer. This timer configures how log after boot-up configuration load, the switch can assume the Primary role from an unresponsive ISL peer and bring up the vLAG ports. The default value is **300**. **Command mode:** Global configuration
no vlag auto-recovery Sets the auto-recovery timer to the default **300** seconds duration. **Command mode:** Global configuration
[no] vlag portchannel *<1-64>* **enable** Enables or disables the vLAG underlying trunk. **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

Table 239. *Virtual Link Aggregation Control Protocol Commands (continued)*

Command Syntax and Usage
`vlag startup-delay` *<0-3600>* Sets the vLAG startup-delay value in seconds to the specified value. The default to `120` seconds. **Note:** Startup delay gives vLAG the ability to prevent traffic loss after a reboot. When a vLAG switch reboots, the vLAG ports are in an errdisabled state. After ISL is up, the vLAG ports are started one by one after the specified startup delay time. This specified time allows the switch to get BGP/OSFP ready through the uplinks so when the vLAG port starts up, all the traffic through those links flows smoothly. Admin status of the ports is honored by the vlag startup delay. For example, if the admin status of the vLAG port is down, those ports will be kept down even after the vLAG start-up delay. **Command mode:** Global configuration
`no vlag startup-delay` Sets the vLAG startup-delay to the default `300` seconds duration. **Command mode:** Global configuration
`[no] vlag tier-id` *<1-512>* Sets the vLAG peer ID. **Command mode:** Global configuration
`show vlag` Display current vLAG configuration. **Command mode:** All

vLAG Health Check Configuration

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

Table 240. *vLAG Health Check Configuration Options*

Command Syntax and Usage
[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 hlthchk peer-ip {*<IP address>***|***<IPv6 address>***}** Configures the IP address of the vLAG peer. **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 241. *vLAG ISL Configuration Options*

Command Syntax and Usage
[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 portchannel *<1-64>* Enables or disables vLAG Inter-Switch Link (ISL) on the selected trunk group. **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 242. *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
`default lacp [system-priority|timeout]` Restores either the VFSM priority value, timeout period or both to their default values. **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
`portchannel` *<trunk ID (*65-128*)>* **`lacp key`** *<1-65535>* Enables a static LACP trunk. In this mode, ports sharing the same LACP admin key can form a single trunk, with the specified `trunk ID`. The active trunk is picked based on the ports which occupy first the trunk ID. Member ports that cannot join this trunk are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic. **Command mode:** Global configuration

Table 242. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
`no portchannel` *<trunk ID (65-128)>* Deletes the specified static LACP trunk. **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 243. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
`lacp key` *<1-65535>* Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group. **Command mode:** Interface port
`lacp mode {off|active|passive}` Set the LACP mode for this port, as follows: o `off` turns LACP off for this port. You can use this port to manually configure a static trunk. o `active` turns LACP on and set this port to active. Active ports initiate LACPDUs. o `passive` turns LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. The default value is `off`. **Command mode:** Interface port
`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 suspend-individual` Sets the port in LACP suspended state if it does not receive LACPDUs anymore. **Note:** The default value is `individual` for internal switch ports and `suspend-individual` for external switch ports. **Command mode:** Interface port

Table 243. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
no lacp suspend-individual Sets the port in LACP individual state if it does not receive LACPDUs anymore. **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
default lacp [key|mode|priority|suspend-individual] Restores the selected parameters to their default values. **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 *Lenovo N/OS Application Guide*.

Table 244. *Layer 2 Failover Configuration Commands*

Command Syntax and Usage
`[no] failover enable` Globally enables or disables Layer 2 Failover. **Command mode:** Global configuration
`[no] failover vlan` Globally turns VLAN monitor `on` or `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. When the VLAN Monitor is `off`, the switch automatically disables all of the internal ports. The default value is `off`. **Command mode:** Global configuration
`show failover trigger [information]` Displays current Layer 2 Failover parameters. **Command mode:** All

Failover Trigger Configuration

The following table displays Failover Trigger configuration commands.

Table 245. *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

The following table displays Auto Monitor configuration commands.

Table 246. *Auto Monitor Configuration Commands*

Command Syntax and Usage
[no] failover trigger *<1-8>* **amon adminkey** *<1-65535>* Adds or removes an 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 portchannel** *<trunk group number>* Adds or removes a trunk group to 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 247. *Failover Manual Monitor Port Commands*

Command Syntax and Usage
[no] failover trigger *<1-8>* **mmon monitor adminkey** *<1-65535>* Adds or removes an LACP *admin key* to the Manual Monitor Port configuration. LACP 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 member** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Port configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon monitor portchannel** *<trunk number>* Adds or removes the selected trunk group to the Manual Monitor Port configuration. **Command mode:** Global configuration
show failover trigger *<1-8>* Displays the current Failover settings. **Command mode:** All

Failover Manual Monitor Control Configuration

Use these commands to define the port link(s) to control. The Manual Monitor Control configuration accepts internal and external ports, but not management ports.

Table 248. *Failover Manual Monitor Control Commands*

Command Syntax and Usage
[no] failover trigger *<1-8>* **mmon control adminkey** *<1-65535>* Adds or removes an LACP *admin key* to the Manual Monitor Control configuration. LACP 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 member** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control portchannel** *<trunk number>* Adds or removes the selected trunk group to the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control vmember** *<UFP vport(s)>* Adds or removes the selected Unified Fabric Port virtual port(s) to the Manual Monitor Control configuration. **Command mode:** Global configuration
show failover trigger *<1-8>* Displays the current Failover settings. **Command mode:** All

Hot Links Configuration

Use these commands to configure Hot Links. For more information about Hot Links, see "Hot Links" in the *Lenovo N/OS 8.2 Application Guide*.

Table 249. *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 enable` Globally enables or disables Hot Links. **Command mode:** Global configuration
`[no] hotlinks fdb-update` Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface. The default value is `disabled`. **Command mode:** Global configuration
`hotlinks fdb-update-rate` *<10-1000>* Configures the FDB Update rate, in packets per second. **Command mode:** Global configuration
`show hotlinks` Displays current Hot Links parameters. **Command mode:** All

Hot Links Trigger Configuration

The following table displays Hot Links Trigger configuration commands.

Table 250. *Hot Links Trigger Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-200>* **enable** Enables or disables the Hot Links trigger. **Command mode:** Global configuration
hotlinks trigger *<1-200>* **forward-delay** *<0-3600>* Configures the Forward Delay interval, in seconds. The default value is `1`. **Command mode:** Global configuration
[no] hotlinks trigger *<1-200>* **name** *<1-32 characters>* Defines a name for the Hot Links trigger. **Command mode:** Global configuration
[no] hotlinks trigger *<1-200>* **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 *<1-200>* Deletes the Hot Links trigger. **Command mode:** Global configuration
show hotlinks trigger *<1-200>* 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 251. *Hot Links Master Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-200>* **master adminkey** *<0-65535>* 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
[no] hotlinks trigger *<1-200>* **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 *<1-200>* **master portchannel** *<trunk group number>* Adds or removes the selected trunk group to the Master interface. **Command mode:** Global configuration
show hotlinks trigger *<1-200>* 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 252. *Hot Links Backup Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-200>* **backup adminkey** *<0-65535>* 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
[no] hotlinks trigger *<1-200>* **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 *<1-200>* **backup portchannel** *<trunk group number>* Adds or removes the selected trunk group to the Backup interface. **Command mode:** Global configuration
show hotlinks trigger *<1-200>* 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.

Up to 4094 VLANs can be configured on the CN4093. VLANs can be assigned any number between 1 and 4094, except the reserved VLANs.

Table 253. *VLAN Configuration Commands*

Command Syntax and Usage
vlan *<VLAN number>* Enter VLAN configuration mode. **Command mode:** Global configuration
[no] cpu Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: o If no Mrouter is present, drop subsequent packets with same IPMC. o If 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] 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 enable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group. **Note**: If both `flood` and `cpu` are disabled, then the switch drops all unregistered IPMC traffic. **Command mode:** VLAN
[no] management Configures this VLAN as a management VLAN. You must have at least one internal port in each new management VLAN. Management port (MGT1) is automatically added to management VLAN. **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

Table 253. *VLAN Configuration Commands (continued)*

Command Syntax and Usage
no name Resets the VLAN name to its default value. **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
protocol-vlan *<1-8>* Configures the Protocol-based VLAN (PVLAN). **Command mode:** VLAN
shutdown Disables local traffic on the specified VLAN. Default setting is enabled (`no shutdown`). **Command mode:** VLAN
no shutdown Enables local traffic on the specified VLAN. Default setting is enabled (`no shutdown`). **Command mode:** VLAN
stg *<STG number>* Assigns a VLAN to a Spanning Tree Group. **Note**: For MST, no VLAN assignation is required. VLANs are mapped from CIST. **Command mode:** VLAN
[no] vmap *<1-128>* **[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
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 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 254. *Protocol VLAN Configuration Commands*

Command Syntax and Usage
[no] protocol-vlan *<1-8>* **enable** Enables or disables the selected protocol on the VLAN. **Command mode:** VLAN
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
[no] protocol-vlan *<1-8>* **member** *<port alias or number>* Adds or removes a port to the selected PVLAN. **Command mode:** VLAN
protocol-vlan *<1-8>* **priority** *<0-7>* Configures the priority value for this PVLAN. **Command mode:** VLAN
protocol-vlan *<1-8>* **protocol** *<protocol type>* Selects a pre-defined protocol, as follows: o `decEther2`: DEC Local Area Transport o `ipv4Ether2`: Internet IP (IPv4) o `ipv6Ether2`: IPv6 o `ipx802.2`: Novell IPX 802.2 o `ipx802.3`: Novell IPX 802.3 o `ipxEther2`: Novell IPX o `ipxSnap`: Novell IPX SNAP o `netbios`: NetBIOS 802.2 o `rarpEther2`: Reverse ARP o `sna802.2`: SNA 802.2 o `snaEther2`: Lenovo SNA Service on Ethernet o `vinesEther2`: Banyan VINES o `xnsEther2`: XNS Compatibility **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 254. *Protocol VLAN Configuration Commands (continued)*

Command Syntax and Usage
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 255. *Private VLAN Configuration Commands*

Command Syntax and Usage
`private-vlan association [add|remove]` *<secondary VLAN list>* Configures Private VLAN mapping between a primary VLAN and secondary VLANs. Enter the primary VLAN ID. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise: o `add` appends the secondary VLANs to the ones currently associated o `remove` excludes the secondary VLANs from the ones currently associated **Command mode:** VLAN
`[no] private-vlan community` Enables or disables the VLAN type as a community VLAN. Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs. **Command mode:** VLAN
`[no] private-vlan isolated` Enables or disables the VLAN type as an isolated VLAN. The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. **Command mode:** VLAN
`[no] private-vlan primary` Enables or disables the VLAN type as a Primary VLAN. A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN. **Command mode:** VLAN
`show vlan private-vlan [type]` Displays private VLAN information. The `type` option lists only the VLAN type for each private VLAN: community, isolated or primary. **Command mode:** All

Layer 3 Configuration

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

Table 256. *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 424. **Command mode:** Global configuration
`ip pim component` *<1-2>* Enters Protocol Independent Multicast (PIM) component configuration mode. To view command options, see page 504. **Command mode:** Global configuration
`ip router-id` *<IP address>* Sets the router ID. **Command mode:** Global configuration
`route-map` *<1-32>* Enter IP Route Map mode. To view command options, see page 433. **Command mode:** Global configuration
`router bgp` Configures Border Gateway Protocol. To view command options, see page 463. **Command mode:** Global configuration
`router ospf` Configures OSPF. To view command options, see page 440. **Command mode:** Global configuration
`router rip` Configures the Routing Interface Protocol. To view command options, see page 437. **Command mode:** Global configuration
`router vrrp` Configures Virtual Router Redundancy. To view command options, see page 490. **Command mode:** Global configuration

Table 256. *Layer 3 Configuration Commands*

Command Syntax and Usage
ipv6 router ospf Enters OSPFv3 configuration mode. To view command options, see page 449. **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 on your network. The Interface option is disabled by default.

IP Interfaces 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 257. *IP Interface Configuration Commands*

Command Syntax and Usage
interface ip *<interface number>* Enter IP interface mode. **Command mode:** Global configuration
[no] enable Enables or disables this IP interface. **Command mode:** Interface IP
ip address *<IP address>* **[***<IP netmask>***]** 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
[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
ipv6 address *<IPv6 address>* **[enable]** **ipv6 address** *<IPv6 address> <IPv6 prefix length (1-128)>* **[enable]** **ipv6 address** *<IPv6 address> <IPv6 prefix length (1-128)>* **anycast [enable]** Configures the IPv6 address of the switch interface, using hexadecimal format with colons. **Command mode:** Interface IP
ipv6 prefixlen *<IPv6 prefix length (1-128)>* Configures the subnet IPv6 prefix length. The default value is `0`. **Command mode:** Interface IP

Table 257. *IP Interface Configuration Commands (continued)*

Command Syntax and Usage
ipv6 secaddr6 address *<IPv6 address> <IPv6 prefix length (1-128)>* **[anycast]** Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons. **Command mode:** Interface IP
no ipv6 secaddr6 Removes the secondary IPv6 address of the switch 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
[no] relay Enables or disables the BOOTP relay on this interface. The default setting is `enabled`. **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 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

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. Default gateway indices are:

- 1-2: Data gateways
- 3: External management gateway
- 4: Internal management gateway

This option is disabled by default.

Table 258. *Default Gateway Configuration Commands*

Command Syntax and Usage
ip gateway *<1-4>* **address** *<IP address>* **[enable]** Configures the IP address of the default IP gateway using dotted decimal notation. The `enable` option also enables the IP gateway for use. **Command mode:** Global configuration
[no] ip gateway *<1-4>* **arp-health-check** Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is `disabled`. **Note:** The `arp` option does not apply to management gateways. **Command mode:** Global configuration
[no] ip gateway *<1-4>* **enable** Enables or disables the gateway for use. **Command mode:** Global configuration
ip gateway *<1-4>* **interval** *<0-60>* The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is `2`. **Command mode:** Global configuration
ip gateway *<1-4>* **retry** *<1-120>* Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is `8` attempts. **Command mode:** Global configuration
no ip gateway *<1-4>* 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 259. *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
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 1. **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, IGMP Snooping/Relay must be enabled, and the required VLANs must be added to IGMP Snooping/Relay.

Table 260. *IP Multicast Route Configuration Commands*

Command Syntax and Usage
[no] ip mroute *<IPMC destination> <VLAN number> <port alias or number>* **{primary|backup|host} [***<virtual router ID>***|none]** Adds or removes a static multicast route. The destination address, VLAN, member port of the route and route type (primary, backup or host) must be specified. **Command mode:** Global configuration
[no] ip mroute *<IP address> <VLAN number>* **adminkey** *<1-65535>* **{primary|backup|host} [***<virtual router ID>***|none]** Adds or removes a static multicast route. The destination address, VLAN, member port of the route and route type (primary, backup or host) must be specified. **Command mode:** Global configuration
[no] ip mroute *<IP address> <VLAN number>* **portchannel** *<trunk group number>* **{primary|backup|host} [***<virtual router ID>***|none]** Adds or removes 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 all Removes all the static multicast routes configured. **Command mode:** Global configuration
show ip mroute Displays the current IP multicast routes. **Command mode:** All

ARP Configuration

Address Resolution Protocol (ARP) is 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 261. *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. **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 262. *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
ip arp *<destination unicast IP address> <destination multicast MAC address>* **vlan** *<cluster vlan number>* Adds a static multicast ARP entry for Network Load Balancing (NLB). **Command mode:** Global configuration
no ip arp [*<IP address>***|all]** Deletes a specific permanent ARP entry or all ARP entries. **Command mode:** Global configuration
show ip arp static Displays current static ARP configuration. **Command mode:** All

IP Forwarding Configuration

The following table displays IP Forwarding configuration commands.

Table 263. *IP Forwarding Configuration Commands*

Command Syntax and Usage
[no] ip routing Enables or disables IP forwarding (routing) on the CN4093. The default setting is `enabled`. **Command mode:** Global configuration
[no] ip routing directed-broadcasts Enables or disables forwarding directed broadcasts. The default setting is `disabled`. **Command mode:** Global configuration
[no] ip routing icmp6-redirect Enables or disables IPv6 ICMP re-directs. The default setting is `disabled`. **Command mode:** Global configuration
[no] ip routing no-icmp-redirect Enables or disables ICMP re-directs. The default setting is `disabled`. **Command mode:** Global configuration
show ip routing Displays the current IP forwarding settings. **Command mode:** All

Network Filter Configuration

The following table displays Network Filter configuration commands.

Table 264. *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`. **Note:** 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.
[no] ip match-address *<1-256>* **enable** Enables or disables the Network Filter configuration. **Command mode:** Global configuration
no ip match-address *<1-256>* Deletes the Network Filter configuration. **Command mode:** Global configuration
show ip match-address [*<1-256>***]** Displays the current the Network Filter configuration. **Command mode:** All

Routing Map Configuration

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

Routing maps control and modify routing information.

Table 265. *Routing Map Configuration Commands*

Command Syntax and Usage
`route-map` *<1-32>* Enter route map configuration mode. **Command mode:** Global configuration
`[no] access-list` *<1-8>* Configures the Access List. For more information, see page 435. **Command mode:** Route map
`[no] as-path-list` *<1-8>* Configures the Autonomous System (AS) Filter. For more information, see page 436. **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] enable` Enables or disables the route map. **Command mode:** Route map
`[no] local-preference` *<0-4294967294>* Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred. **Command mode:** Route map
`[no] metric` *<1-4294967294>* Sets the metric of the matched route. **Command mode:** Route map
`[no] metric-type {1|2}` Assigns the type of OSPF metric. The default is type 1. o `Type 1`—External routes are calculated using both internal and external metrics. o `Type 2`—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2. o `none`—Removes the OSPF metric. **Command mode:** Route map

Table 265. *Routing Map Configuration Commands (continued)*

Command Syntax and Usage
precedence *<1-255>* Sets the precedence of the route map. The smaller the value, the higher the precedence. The default value is **10**. **Command mode:** Route map
[no] weight *<0-65534>* Sets the weight of 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 266. *IP Access List Configuration Commands*

Command Syntax and Usage
access-list *<1-8>* **action {permit|deny}** Permits or denies action for the access list. **Command mode:** Route map
[no] access-list *<1-8>* **enable** Enables or disables the access list. **Command mode:** Route map
[no] access-list *<1-8>* **match-address** *<1-256>* Sets the network filter number. See "Network Filter Configuration" on page 432 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
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 267. *AS Filter Configuration Commands*

Command Syntax and Usage
as-path-list *<1-8>* **action {permit|deny}** Permits or denies Autonomous System filter action. **Command mode:** Route map
as-path-list *<1-8>* **as-path** *<1-65535>* Sets the Autonomous System filter's path number. **Command mode:** Route map
[no] as-path-list *<1-8>* **enable** Enables or disables the Autonomous System filter. **Command mode:** Route map
no as-path-list *<1-8>* Deletes the Autonomous System filter. **Command mode:** Route map
show route-map *<1-32>* **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 268. *Routing Information Protocol Commands*

Command Syntax and Usage
router rip Enter Router RIP configuration mode. **Command mode:** Global Configuration
[no] enable Globally enables or disables RIP. **Command mode:** Router RIP
timers update *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is **30**. **Command mode:** Router RIP
show ip rip Displays the current RIP configuration. **Command mode:** All

RIP Interface Configuration

The RIP Interface commands are used for configuring Routing Information Protocol parameters for the selected interface.

Note: Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 269. *RIP Interface Commands*

Command Syntax and Usage
[no] ip rip authentication key *<password>* Configures the authentication key password. **Command mode:** Interface IP
[no] ip rip authentication type [*<password>***]** Configures the authentication type. The default is none. **Command mode:** Interface IP

Table 269. *RIP Interface Commands (continued)*

Command Syntax and Usage
[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 enable Enables or disables this RIP interface. **Command mode:** Interface IP
[no] ip rip listen When enabled, the switch learns routes from other routers. The default value is `enabled`. **Command mode:** Interface IP
[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 multicast-updates Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is `enabled`. **Command mode:** Interface IP
[no] ip rip poison When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is `disabled`. **Command mode:** Interface IP
[no] ip rip split-horizon Enables or disables split horizon. The default value is `enabled`. **Command mode:** Interface IP
[no] ip rip supply When enabled, the switch supplies routes to other routers. The default value is `enabled`. **Command mode:** Interface IP

Table 269. *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
ip rip version {1|2|both} Configures the RIP version used by this interface. The default value is `version 2`. **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 270. *RIP Redistribution Commands*

Command Syntax and Usage
[no] redistribute {fixed|static|ospf|eospf|ebgp|ibgp} *<1-32>* Adds or removes the selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (,). To add or removes 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
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. **Command mode:** Router RIP
no redistribute {fixed|static|ospf|eospf|ebgp|ibgp} export Stops exporting the routes of the protocol. **Command mode:** RIP
show ip rip redistribute Displays the current RIP route redistribute configuration. **Command mode:** All

Open Shortest Path First Configuration

The following table describes the OSPF commands.

Table 271. *OSPF Configuration Commands*

Command Syntax and Usage
router ospf Enter Router OSPF configuration mode. **Command mode:** Global configuration
ip ospf *<interface number>* Configures the OSPF interface. See page 444 to view command options. **Command mode:** Interface IP
area *<0-2>* Configures the OSPF area index. See page 441 to view command options. **Command mode:** Router OSPF
area-virtual-link *<1-3>* Configures the Virtual Links used to configure OSPF for a Virtual Link. See page 446 to view command options. **Command mode:** Router OSPF
area-range *<1-16>* Configures summary routes for up to 16 IP addresses. See page 443 to view command options. **Command mode:** Router OSPF
default-information *<1-16777214> <AS external metric type (1-2)>* Sets one default route among multiple choices in an area. **Command mode:** Router OSPF
no default-information Removes the default route information. **Command mode:** Router OSPF
[no] enable Enables or disables OSPF on the CN4093. **Command mode:** Router OSPF
host *<1-128>* Configures OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 447 to view command options. **Command mode:** Router OSPF

Table 271. *OSPF Configuration Commands (continued)*

Command Syntax and Usage
lsdb-limit *<LSDB limit (0-2048, 0 for no limit)>* Sets the link state database limit. **Command mode:** Router OSPF
message-digest-key *<1-255>* **md5-key** *<text string>* Assigns a string to MD5 authentication key. **Command mode:** Router OSPF
redistribute Configures OSPF route redistribution. See page 448 to view command options. **Command mode:** Router OSPF
show ip ospf Displays the current OSPF configuration settings. **Command mode:** All

Area Index Configuration

The following table describes the Area Index commands.

Table 272. *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
[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
[no] area *<0-2>* **enable** Enables or disables the OSPF area. **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. **Command mode:** Router OSPF

Table 272. *Area Index Configuration Commands*

Command Syntax and Usage
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
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. **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

The following table describes the OSPF Summary Range commands.

Table 273. *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>* **enable** Enables or disables the OSPF summary range. **Command mode:** Router OSPF
[no] area-range *<1-16>* **hide** Hides or shows the OSPF summary range. **Command mode:** Router OSPF
no area-range *<1-16>* Deletes the OSPF summary range. **Command mode:** Router OSPF
show ip ospf area-range *<1-16>* Displays the current OSPF summary range. **Command mode:** Router OSPF

OSPF Interface Configuration

The following table describes the OSPF Interface commands.

Table 274. *OSPF Interface Configuration Commands*

Command Syntax and Usage
ip ospf area *<0-2>* Configures the OSPF area index. **Command mode:** Interface IP
ip ospf cost *<1-65535>* Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. **Command mode:** Interface IP
ip ospf dead-interval *<1-65535>* **ip ospf dead-interval** *<1000-65535ms>* Configures the health parameters of a `hello` packet, in seconds or milliseconds, before declaring a silent router to be `down`. **Command mode:** Interface IP
[no] ip ospf enable Enables or disables OSPF interface. **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
[no] ip ospf message-digest-key *<1-255>* Assigns an MD5 key to the interface. **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 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

Table 274. *OSPF Interface Configuration Commands (continued)*

Command Syntax and Usage
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
ip ospf retransmit-interval *<1-3600>* Configures the retransmit interval in seconds. **Command mode:** Interface IP
ip ospf transit-delay *<1-3600>* Configures the transit delay in seconds. **Command mode:** Interface IP
no ip ospf Deletes the OSPF interface. **Command mode:** Interface IP
show interface ip *<interface number>* **ospf** Displays the current settings for OSPF interface. **Command mode:** All

OSPF Virtual Link Configuration

The following table describes the OSPF Virtual Link commands.

Table 275. *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>* **dead-interval** *<1-65535>* **area-virtual-link** *<1-3>* **dead-interval** *<1000-65535ms>* Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is **40**. **Command mode:** Router OSPF
[no] area-virtual-link *<1-3>* **enable** Enables or disables OSPF virtual link. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **hello-interval** *<1-65535>* **area-virtual-link** *<1-3>* **hello-interval** *<50-65535ms>* Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is **10**. **Command mode:** Router OSPF
[no] area-virtual-link *<1-3>* **key** *<password>* Configures the password (up to eight characters) for each virtual link. The default setting is none. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **message-digest-key** *<1-255>* Sets MD5 key ID for each virtual link. The default setting is none. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **neighbor-router** *<IP address>* Configures the router ID of the virtual neighbor. The default value is **0.0.0.0**. **Command mode:** Router OSPF
area-virtual-link *<1-3>* **retransmit-interval** *<1-3600>* Configures the retransmit interval, in seconds. The default value is **5**. **Command mode:** Router OSPF

Table 275. *OSPF Virtual Link Configuration Commands (continued)*

Command Syntax and Usage
area-virtual-link *<1-3>* **transit-delay** *<1-3600>* Configures the delay in transit, in seconds. The default value is **1**. **Command mode:** Router OSPF
no area-virtual-link *<1-3>* Deletes OSPF virtual link. **Command mode:** Router OSPF
show ip ospf area-virtual-link *<1-3>* Displays the current OSPF virtual link settings. **Command mode:** All

OSPF Host Entry Configuration

The following table describes the OSPF Host Entry commands.

Table 276. *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
[no] host *<1-128>* **enable** Enables or 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

The following table describes the OSPF Route Redistribution commands.

Table 277. *OSPF Route Redistribution Configuration Commands*

Command Syntax and Usage
[no] redistribute {fixed|static|rip|ebgp|ibgp} *<rmap ID (1-32)>* Adds or removes selected routing map to the rmap list. This option adds or removes 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} export metric *<1-16777214>* **metric-type {type1|type2}** Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none. **Command mode:** Router OSPF
show ip ospf redistribute Displays the current route map settings. **Command mode:** All

OSPF MD5 Key Configuration

The following table describes the OSPF MD5 Key commands.

Table 278. *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

Open Shortest Path First Version 3 Configuration

The following table describes the OSPFv3 commands.

Table 279. *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: o Standard o Cisco o 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
`[no] enable` Enables or disables OSPFv3 on the switch. **Command mode**: Router OSPF3
`exit-overflow-interval` *<0-4294967295>* Configures the number of seconds that a router takes to exit Overflow State. The default value is `0`. **Command mode**: Router OSPF3
`[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 279. *OSPFv3 Configuration Commands (continued)*

Command Syntax and Usage
neighbor *<1-256>* **{address** *<IPv6 address>***|enable|interface** *<1-126>***| |priority** *<0-255>***}** Configures directly reachable routers over non-broadcast networks.This is required for non-broadcast multiple access (NBMA) networks and optional for Point-to-Multipoint networks. o `address` configures the neighbor's IPv6 address. o `enable` activates a previously disabled neighbor. o `interface` configures the OSPFv3 interface used for the neighbor entry. o `priority` configures the priority value used for the neighbor entry. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the neighbor cannot be used as Designated Router. The default value is `1`. **Command mode**: Router OSPF3
no neighbor *<1-256>* **[enable]** Deletes the neighbor entry. Using the `enable` option only disables the neighbor, while preserving it's settings. **Command mode**: Router OSPF3
reference-bandwidth *<0-4294967295>* Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is `100,000`. **Command mode**: Router OSPF3
router-id *<IPv4 address>* Defines the router ID. **Command mode**: Router OSPF3
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
show ipv6 ospf Displays the current OSPF configuration settings. **Command mode**: All

OSPFv3 Area Index Configuration

The following table describes the OSPFv3 Area Index commands.

Table 280. *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>* **default-metric** *<metric value (1-16777215)>* Configures the cost for the default summary route in a stub area or NSSA. **Command mode**: Router OSPF3
area *<area index>* **default-metric type** *<1-3>* Configures the default metric type applied to the route. **Note:** This command applies only to area type of Stub/NSSA. **Command mode**: Router OSPF3
[no] area *<area index>* **enable** Enables or disables the OSPF area. **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: o `always`: Type 7 LSAs are always translated into Type 5 LSAs. o `candidate`: An NSSA border router participates in the translator election process. The default setting is `candidate`. **Command mode**: Router OSPF3

Table 280. *OSPFv3 Area Index Configuration Options (continued)*

Command Syntax and Usage
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
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

The following table describes the OSPFv3 Summary Range commands.

Table 281. *OSPFv3 Summary Range Configuration Options*

Command Syntax and Usage
area-range *<1-16>* **address** *<IPv6 address> <prefix length (1-128)>* Configures the base IPv6 address and subnet prefix length for the range. **Command mode**: Router OSPF3
area-range *<1-16>* **area** *<area index (0-2)>* Configures the area index used by the switch. **Command mode**: Router OSPF3
[no] area-range *<1-16>* **enable** Enables or disables the OSPFv3 summary range. **Command mode**: Router OSPF3
[no] area-range *<1-16>* **hide** Hides or shows the OSPFv3 summary range. **Command mode**: Router OSPF3
area-range *<1-16>* **lsa-type {summary|Type7}** Configures the LSA type, as follows: o Summary LSA o Type7 LSA **Command mode**: Router OSPF3
area-range *<1-16>* **tag** *<0-4294967295>* Configures the route tag. **Command mode**: Router OSPF3
no area-range *<1-16>* Deletes the OSPFv3 summary range. **Command mode**: Router OSPF3
show ipv6 ospf area-range Displays the current OSPFv3 summary range. **Command mode**: All

OSPFv3 AS-External Range Configuration

The following table describes the OSPFv3 AS-External Range commands.

Table 282. *OSPFv3 AS-External Range Configuration Options*

Command Syntax and Usage
summary-prefix *<1-16>* **address** *<IPv6 address> <IPv6 prefix length (1-128)>* Configures the base IPv6 address and the subnet prefix length for the range. **Command mode**: Router OSPF3
summary-prefix *<1-16>* **aggregation-effect {allowAll|denyAll| |advertise|not-advertise}** Configures the aggregation effect, as follows: – `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
summary-prefix *<1-16>* **area** *<area index (0-2)>* Configures the area index used by the switch. **Command mode**: Router OSPF3
[no] summary-prefix *<1-16>* **enable** Enables or disables the OSPFv3 AS-external range. **Command mode**: Router OSPF3
[no] summary-prefix *<1-16>* **translation** When `enabled`, the P-bit is set in the generated Type-7 LSA. When `disabled`, the P-bit is cleared. The default setting is `disabled`. **Command mode**: Router OSPF3
no summary-prefix *<1-16>* Deletes the OSPFv3 AS-external range. **Command mode**: Router OSPF3
show ipv6 ospf summary-prefix *<1-16>* Displays the current OSPFv3 AS-external range. **Command mode**: All

OSPFv3 Interface Configuration

The following table describes the OSPFv3 Interface commands.

Table 283. *OSPFv3 Interface Configuration Options*

Command Syntax and Usage
interface ip *<interface number>* Enter Interface IP mode, from Global Configuration mode. **Command mode**: Global configuration
[no] ipsec dynamic-policy *<1-10>* Adds or removes an IP security dynamic policy to the OSPFv3 interface. **Command mode**: Interface IP
[no] ipsec manual-policy *<1-10>* Adds or removes an IP security manual policy to the OSPFv3 interface. **Command mode**: Interface IP
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 cost *<1-65535>* Configures the metric value for sending a packet 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 enable Enables or disables OSPFv3 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

Table 283. *OSPFv3 Interface Configuration Options (continued)*

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

Table 283. *OSPFv3 Interface Configuration Options (continued)*

Command Syntax and Usage
[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 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 284. *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
ipv6 ospf authentication ipsec enable Enables IPsec authentication. **Command mode:** Interface IP
ipv6 ospf authentication ipsec spi *<256-4294967295>* **{md5|sha1}** *<authentication key (hexadecimal)>* Configures the Security Parameters Index (SPI), algorithm, and authentication key for the Authentication Header (AH). The algorithms supported are: o MD5 (hexadecimal key length is 32) o SHA1 (hexadecimal key length is 40) **Command mode:** Interface IP
ipv6 ospf authentication ipsec default Resets the Authentication Header (AH) configuration to default values. **Command mode:** Interface IP
no ipv6 ospf authentication ipsec spi *<256-4294967295>* Disables the specified Authentication Header (AH) SPI. **Command mode:** Interface IP

Table 284. *Layer 3 IPsec Configuration Options (continued)*

Command Syntax and Usage
ipv6 ospf encryption ipsec enable Enables OSPFv3 encryption for this interface. **Command mode:** Interface IP
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: o `3DES` (hexadecimal key length is 48) o `AES-CBC` (hexadecimal key length is 32) o `DES` (hexadecimal key length is 16) The authentication algorithms supported are: o `MD5` (hexadecimal key length is 32) o `SHA1` (hexadecimal key length is 40) o `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 default Resets the Encapsulating Security Payload (ESP) configuration to default values. **Command mode:** Interface IP
no ipv6 ospf encryption ipsec spi *<256-4294967295>* Disables the specified Encapsulating Security Payload (ESP) SPI. **Command mode:** Interface IP

OSPFv3 Virtual Link Configuration

The following table describes the OSPFv3 Virtual Link commands.

Table 285. *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>* **dead-interval** *<1-65535>* Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down. **Command mode**: Router OSPF3
[no] area-virtual-link *<1-3>* **enable** Enables or disables OSPF virtual link. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **hello-interval** *<1-65535)>* Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **neighbor-router** *<NBR router ID (IP address)>* Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0. **Command mode**: Router OSPF3
area-virtual-link *<1-3>* **retransmit-interval** *<1-1800>* 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>* **transmit-delay** *<1-1800>* Configures the estimated time, in seconds, taken to transmit LS update packet over this interface. **Command mode**: Router OSPF3
no area-virtual-link *<1-3>* Deletes OSPF virtual link. **Command mode**: Router OSPF3
show ipv6 ospf area-virtual-link Displays the current OSPFv3 virtual link settings. **Command mode**: All

OSPFv3 over IPSec for Virtual Link Configuration

The following table describes the OSPFv3 over IPsec for Virtual Link Configuration commands.

Table 286. *Layer 3 IPsec Configuration Options*

Command Syntax and Usage
area-virtual-link *<1-3>* **authentication ipsec {default|enable|spi** *<256-4294967295>***}** Sets OSPFv3 authentication mode. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **authentication ipsec spi** *<256-4294967295>* **{md5** *<md5 key>***|sha1** *<sha1 key>***}** Configures the OSPFv3 security parameter index authentication. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **encryption ipsec {default|enable| |spi** *<256-4294967295>***}** Sets OSPFv3 encryption. **Command mode:** Router OSPF3
area-virtual-link *<1-3>* **encryption ipsec spi** *<256-4294967295>* **esp {3des** *<3des key>***|aes-cbc** *<aes-cbc key>***|null} {md5|none|sha1}** Configures the OSPFv3 security parameter index encryption. **Command mode:** Router OSPF3
show ipv6 ospf area-virtual-link Displays the current OSPFv3 virtual link settings. **Command mode**: All

OSPFv3 Host Entry Configuration

The following table describes the OSPFv3 Host Entry commands.

Table 287. *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
[no] host *<1-128>* **enable** Enables or disables the host entry. **Command mode**: Router OSPF3
no host *<1-128>* Deletes the host entry. **Command mode**: Router OSPF3
show ipv6 ospf host [*<1-128>***]** Displays the current OSPFv3 host entries. **Command mode**: All

OSPFv3 Redistribute Entry Configuration

The following table describes the OSPFv3 Redistribute Entry commands.

Table 288. *OSPFv3 Redist Entry Configuration Options*

Command Syntax and Usage
redist-config *<1-128>* **address** *<IPv6 address> <IPv6 prefix length (1-128)>* Configures the base IPv6 address and the subnet prefix length for the redistribution entry. **Command mode**: Router OSPF3
[no] redist-config *<1-128>* **enable** Enables or disables the OSPFv3 redistribution entry. **Command mode**: Router OSPF3

Table 288. *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
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
[no] redist-config *<1-128>* **tag** *<0-4294967295>* Configures the route tag. **Command mode**: Router OSPF3
no redist-config *<1-128>* Deletes the OSPFv3 redistribution entry. **Command mode**: Router OSPF3
show ipv6 ospf redist-config Displays the current OSPFv3 redistribution configuration entries. **Command mode**: Router OSPF3

OSPFv3 Redistribute Configuration

The following table describes the OSPFv3 Redistribute commands.

Table 289. *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

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 Lenovo N/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 290. *Border Gateway Protocol Commands*

Command Syntax and Usage
router bgp Enter Router BGP configuration mode. **Command mode:** Global configuration
as *<0-65535>* Set Autonomous System number. **Command mode:** Router BGP
[no] asn4comp Enables or disables ASN4 to ASN2 compatibility. **Command mode:** Router BGP
[no] enable Globally enables or disables BGP. **Command mode:** Router BGP
local-preference *<0-4294967294>* Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP. **Command mode:** Router BGP

Table 290. *Border Gateway Protocol Commands (continued)*

Command Syntax and Usage
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 464. **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 291. *BGP Peer Configuration Commands*

Command Syntax and Usage
neighbor *<1-12>* **advertisement-interval** *<1-65535>* Sets time, in seconds, between advertisements. The default value is **60**. **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
[no] neighbor *<1-12>* **password** *<1-16 characters>* Configures the BGP peer password. **Command mode:** Router BGP
neighbor *<peer numer (1-12)>* **redistribute** Configures BGP neighbor redistribution. To view command options, see page 468. **Command mode:** Router BGP
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

Table 291. *BGP Peer Configuration Commands (continued)*

Command Syntax and Usage
neighbor *<1-12>* **remote-as** *<1-65535>* Sets the remote autonomous system number for the specified peer. **Command mode:** Router BGP
neighbor *<1-12>* **retry-interval** *<1-65535>* Sets connection retry interval, in seconds. The default value is **120**. **Command mode:** Router BGP
[no] neighbor *<1-12>* **route-map in** *<1-32>* Adds or removes route map into in-route map list. **Command mode:** Router BGP
[no] neighbor *<1-12>* **route-map out** *<1-32>* Adds or removes route map into out-route map list. **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**. **Command mode:** Router BGP
neighbor *<1-12>* **shutdown** Disables this peer configuration. **Command mode:** Router BGP
no neighbor *<1-12>* **shutdown** Enables this peer configuration. **Command mode:** Router BGP

Table 291. *BGP Peer Configuration Commands (continued)*

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

BGP Aggregation Configuration

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

Table 292. *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
[no] aggregate-address *<1-16>* **enable** Enables or disables this BGP aggregation. **Command mode:** Router BGP
no aggregate-address *<1-16>* Deletes this BGP aggregation. **Command mode:** Router BGP
show ip bgp aggregate-address [*<1-16>***]** Displays the current BGP aggregation configuration. **Command mode:** All

BGP Neighbor Redistribution Configuration

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

Table 293. *BGP Redistribution Configuration Commands*

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

Multicast Listener Discovery Protocol Configuration

Table 294 describes the commands used to configure MLD parameters.

Table 294. *MLD Protocol 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
[no] enable Globally enables or disables MLD. **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 295 describes the commands used to configure MLD parameters for an interface.

Table 295. *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
[no] ipv6 mld enable Enables or disables this MLD interface. **Command mode:** Interface IP

Table 295. *MLD Interface Configuration Commands (continued)*

Command Syntax and Usage
ipv6 mld llistnr *<1-32>* Configures the Last Listener query interval, in seconds. The default value is 1. **Command mode:** Interface IP
ipv6 mld qintrval *<2-65535>* Configures the interval for MLD Query Reports, in seconds. The default value is 125. **Command mode:** Interface IP
ipv6 mld qri *<1000-65535>* Configures the interval for MLD Query Response Reports, in miliseconds. The default value is 10,000. **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 296 describes the commands used to configure basic IGMP parameters.

Table 296. *IGMP Configuration Commands*

Command Syntax and Usage
`[no] ip igmp aggregate` Enables or disables IGMP Membership Report aggregation. **Command mode**: Global configuration
`[no] ip igmp enable` Globally enables or disables IGMP. **Command mode:** Global configuration
`show ip igmp` Displays the current IGMP configuration parameters. **Command mode:** All

The following sections describe the IGMP configuration options.

IGMP Snooping Configuration

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 297 describes the commands used to configure IGMP Snooping.

Table 297. *IGMP Snooping Configuration Commands*

Command Syntax and Usage
`[no] ip igmp snoop enable` Enables or disables IGMP Snooping. **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
`[no] ip igmp snoop vlan` *<VLAN number>* Adds or removes the selected VLAN(s) to 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 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`. **Command mode:** Global configuration
`show ip igmp snoop` Displays the current IGMP Snooping parameters. **Command mode:** All

IGMPv3 Configuration

Table 298 describes the commands used to configure IGMP version 3.

Table 298. *IGMP version 3 Configuration Commands*

Command Syntax and Usage
`[no] ip igmp snoop igmpv3 enable` Enables or disables IGMP version 3. The default setting is `disabled`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 exclude` Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default setting is `enabled`. **Command mode:** Global configuration
`ip igmp snoop igmpv3 sources` *<1-64>* Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is `8`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 v1v2` Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default setting is `enabled`. **Command mode:** Global configuration
`show ip igmp snoop igmpv3` Displays the current IGMP v3 Snooping configuration. **Command mode:** All

IGMP Relay Configuration

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

Table 299 describes the commands used to configure IGMP Relay.

Table 299. *IGMP Relay Configuration Commands*

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

IGMP Filtering Configuration

Table 300 describes the commands used to configure an IGMP filter.

Table 300. *IGMP Filtering Configuration Commands*

Command Syntax and Usage
`ip igmp profile` *<1-16>* Configures the IGMP filter. To view command options, see page 475. **Command mode:** Global configuration
`[no] ip igmp filtering` Enables or disables IGMP filtering globally. **Command mode:** Global configuration
`show ip igmp filtering` Displays the current IGMP Filtering parameters. **Command mode:** All

IGMP Filter Definition

Table 301 describes the commands used to define an IGMP filter.

Table 301. *IGMP Filter Definition Commands*

Command Syntax and Usage
ip igmp profile *<1-16>* **action {allow|deny}** Allows or denies multicast traffic for the IP multicast addresses specified. The default action is deny. **Command mode:** Global configuration
[no] ip igmp profile *<1-16>* **enable** Enables or disables this IGMP filter. **Command mode:** Global configuration
ip igmp profile *<1-16>* **range** *<IP address 1> <IP address 2>* Configures the range of IP multicast addresses for this filter. **Command mode:** Global configuration
no ip igmp profile *<1-16>* Deletes this filter's parameter definitions. **Command mode:** Global configuration
show ip igmp profile *<1-16>* Displays the current IGMP filter. **Command mode:** All

IGMP Filtering Port Configuration

Table 302 describes the commands used to configure a port for IGMP filtering.

Table 302. *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
[no] ip igmp profile *<1-16>* Adds or removes an IGMP filter to this port. **Command mode:** Interface port
show interface port *<port alias or number>* **igmp-filtering** Displays the current IGMP filter parameters for this port. **Command mode:** All

IGMP Relay Multicast Router Configuration

Table 303 describes the commands used to configure multicast routers for IGMP Relay.

Table 303. *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>* **attempt** *<1-128>* Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5. **Command mode:** Global configuration
[no] ip igmp relay mrouter *<1-2>* **enable** Enables or disables the multicast router. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **interval** *<1-60>* Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **retry** *<1-120>* Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4. **Command mode:** Global configuration
ip igmp relay mrouter *<1-2>* **version** *<1-2>* Configures the IGMP version (1 or 2) of the multicast router. **Command mode:** Global configuration
no ip igmp relay mrouter *<1-2>* Deletes the multicast router from IGMP Relay. **Command mode:** Global configuration
show ip igmp relay Displays the current IGMP Relay configuration. **Command mode:** All

IGMP Static Multicast Router Configuration

Table 304 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 304. *IGMP Static Multicast Router Configuration Commands*

Command Syntax and Usage
ip igmp mrouter port *<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, 2 or 3) of the multicast router. **Command mode:** Global configuration
no ip igmp mrouter port *<port alias or number> <VLAN number> <version (1-3)>* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
no ip igmp mrouter all Removes all static multicast routers. **Command mode:** Global configuration
clear ip igmp mrouter Clears the Dynamic router port table. **Command mode:** Global configuration
show ip igmp mrouter Displays the current IGMP Static Multicast Router parameters. **Command mode:** All

IGMP Advanced Configuration

Table 305 describes the commands used to configure advanced IGMP parameters.

Table 305. *IGMP Advanced Configuration Commands*

Command Syntax and Usage
`[no] ip igmp fastleave` *<VLAN number>* Enables or disables Fastleave processing. Fastleave lets the switch immediately remove a port from the IGMP port list if the host sends a Leave message and the proper conditions are met. The default setting is `disabled`. **Command mode:** Global configuration
`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` *<1-10>* Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If you expect the subnet to have a high rate of packet loss, increase the value. The default value is `2`. **Command mode:** Global configuration
`[no] ip igmp rtralert` Enables or disables the Router Alert option in IGMP messages. **Command mode:** Global configuration
`ip igmp timeout` *<1-255>* Configures the Query Response Interval. This is a value used to determine the Group Membership Interval, together with the Robustness Variable and the Query Interval. The range is from 1 to 255 seconds. The default value is `10`. **Command mode:** Global configuration

IGMP Querier Configuration

Table 306. describes the commands used to configure IGMP Querier.

Table 306. *IGMP Querier Configuration Options*

Command Syntax and Usage
`[no] ip igmp querier enable` Globally enables or disables IGMP Querier. **Command mode:** Global configuration
`[no] ip igmp querier vlan` *<VLAN number>* **`enable`** Enables or disables the IGMP Querier for the specified VLAN. **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>* **`max-response`** *<1-256>* Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message.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. The default value is `100`. **Command mode:** Global configuration
`ip igmp querier vlan` *<VLAN number>* **`query-interval`** *<1-608>* Configures the interval between IGMP Query broadcasts, in seconds. The default value is `125`. **Command mode:** Global configuration
`ip igmp querier vlan` *<VLAN number>* **`robustness`** *<1-10>* Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is `2`. **Command mode:** Global configuration
`ip igmp querier vlan` *<VLAN number>* **`source-ip`** *<IP address>* Configures the IGMP source IP address for the selected VLAN. **Command mode:** Global configuration

Table 306. *IGMP Querier Configuration Options (continued)*

Command Syntax and Usage
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>* **startup-interval** *<1-608>* Configures the Startup Query Interval, which is the interval between General Queries sent out at startup. The default value is 31 seconds. **Command mode:** Global configuration
ip igmp querier vlan *<VLAN number>* **version [v1|v2|v3]** Configures the IGMP version. The default version is v3. **Command mode:** Global configuration
show ip igmp querier Displays the current IGMP Querier parameters. **Command mode:** All
show ip igmp querier vlan *<VLAN number>* Displays IGMP Querier information for the selected VLAN. **Command mode:** Global configuration

IKEv2 Configuration

Table 307 describes the commands used to configure IKEv2.

Table 307. *IKEv2 Options*

Command Syntax and Usage
`[no] ikev2 cookie` Enables or disables cookie notification. **Command mode:** Global configuration
`ikev2 retransmit-interval` *<1-20>* Sets the interval, in seconds, the timeout value in case a packet is not received by the peer and needs to be retransmitted. The default value is `20`. **Command mode:** Global configuration
`show ikev2` Displays the current IKEv2 settings. **Command mode:** All

IKEv2 Proposal Configuration

Table 308 describes the commands used to configure an IKEv2 proposal.

Table 308. *IKEv2 Proposal Options*

Command Syntax and Usage
`ikev2 proposal` Enter IKEv2 proposal mode. **Command mode:** Global configuration
`encryption {3des|aes-cbc}` Configures IKEv2 encryption mode. The default value is `3des`. **Command mode:** IKEv2 proposal
`group {`*1*`|`*2*`|`*5*`|`*14*`|`*24*`}`** Configures the the DH group. The default group is `24`. **Command mode:** IKEv2 proposal
`integrity {md5|sha1}` Configures the IKEv2 authentication algorithm type. The default value is `sha1`. **Command mode:** IKEv2 proposal

IKEv2 Preshare Key Configuration

Table 309 describes the commands used to configure IKEv2 preshare keys.

Table 309. *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 310 describes the commands used to configure IKEv2 identification.

Table 310. *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 email *<1-32 characters>* Configures the switch to use the supplied email address (such as "`xyz@example.com`") 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
show ikev2 identity Displays the current IKEv2 identification settings. **Command mode:** All

IPsec Configuration

Table 311 describes the commands used to configure IPsec.

Table 311. *IPsec Options*

Command Syntax and Usage
[no] ipsec enable Enables or disables IPsec. **Command mode:** Global configuration
show ipsec Displays the current IPsec settings. **Command mode:** All

IPsec Transform Set Configuration

Table 312 describes the commands used to configure IPsec transforms.

Table 312. *IPsec Transform Set Options*

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

Table 312. *IPsec Transform Set Options (continued)*

Command Syntax and Usage
no ipsec transform *<1-10>* Deletes the transform set. **Command mode:** Global configuration
show ipsec transform-set *<1-10>* Displays the current IPsec Transform Set settings. **Command mode:** All

IPsec Traffic Selector Configuration

Table 313 describes the commands used to configure an IPsec traffic selector.

Table 313. *IPsec Traffic Selector Options*

Command Syntax and Usage
ipsec traffic-selector *<1-10>* **{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
no ipsec traffic-selector *<1-10>* Resets the specified traffic selector to its default settings. **Command mode:** Global configuration

IPsec Dynamic Policy Configuration

Table 314 describes the commands used to configure an IPsec dynamic policy.

Table 314. *IPsec Dynamic Policy Options*

Command Syntax and Usage
ipsec dynamic-policy *<1-10>* Enter IPsec dynamic policy mode. **Command mode:** Global configuration
peer *<IPv6 address>* Sets the remote peer IP address. **Command mode:** IPsec dynamic policy
pfs {enable|disable} Enables/disables perfect forward security. **Command mode:** IPsec dynamic policy

Table 314. *IPsec Dynamic Policy Options (continued)*

Command Syntax and Usage
sa-lifetime *<120-86400>* Sets the IPsec SA lifetime in seconds. The default value is 86400. **Command mode:** IPsec dynamic policy
traffic-selector *<1-10>* Sets the traffic selector for the IPsec policy. **Command mode:** IPsec dynamic policy
transform-set *<1-10>* Sets the transform set for the IPsec policy. **Command mode:** IPsec dynamic policy
show ipsec dynamic-policy *<1-10>* Displays the current IPsec dynamic policy settings. **Command mode:** All

IPsec Manual Policy Configuration

Table 315 describes the commands used to configure an IPsec manual policy.

Table 315. *IPsec Manual Policy Options*

Command Syntax and Usage
ipsec manual-policy *<1-10>* Enter IPsec manual policy mode. **Command mode:** Global configuration
in-ah auth-key *<key code (hexadecimal)>* Sets inbound Authentication Header (AH) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
in-ah spi *<256-4294967295>* Sets the inbound Authentication Header (AH) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy

Table 315. *IPsec Manual Policy Options (continued)*

Command Syntax and Usage
in-esp auth-key *<key code (hexadecimal)>* Sets the inbound Encapsulating Security Payload (ESP) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy
in-esp cipher-key *<key code (hexadecimal)>* Sets the inbound Encapsulating Security Payload (ESP) cipher key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy
in-esp spi *<256-4294967295>* Sets the inbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
out-ah auth-key *<key code (hexadecimal)>* Sets the outbound Authentication Header (AH) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
out-ah spi *<256-4294967295>* Sets the outbound Authentication Header (AH) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
out-esp auth-key *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy

Table 315. *IPsec Manual Policy Options (continued)*

Command Syntax and Usage
out-esp cipher-key *<key code (hexadecimal)>* Sets the outbound Encapsulating Security Payload (ESP) cipher key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption. **Command mode:** IPsec manual policy
out-esp spi *<256-4294967295>* Sets the outbound Encapsulating Security Payload (ESP) Security Parameter Index (SPI). **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption. **Command mode:** IPsec manual policy
peer *<IPv6 address>* Sets the remote peer IP address. **Command mode:** IPsec manual policy
traffic-selector *<1-10>* Sets the traffic selector for the IPsec policy. **Command mode:** IPsec manual policy
transform-set *<1-10>* Sets the transform set for the IPsec policy. **Command mode:** IPsec manual policy
show ipsec manual-policy *<1-10>* Displays the current IPsec manual policy settings. **Command mode:** All

Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 316. *Domain Name Service Commands*

Command Syntax and Usage
`[no] ip dns domain-name` *<string>* Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
`[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: o IPv4 o IPv6 **Command mode:** Global configuration
`show ip dns` Displays the current Domain Name System settings. **Command mode:** All

Bootstrap Protocol Relay Configuration

The Bootstrap Protocol (BOOTP) Relay commands are used to let hosts get 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 317. *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
[no] ip bootp-relay enable Globally enables or disables BOOTP relay. **Command mode:** Global configuration

BOOTP Relay Broadcast Domain Configuration

These commands allow you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

Table 318. *BOOTP Relay Broadcast Domain Configuration Options*

Command Syntax and Usage
[no] ip bootp-relay bcast-domain *<1-10>* **enable** Enables or disables BOOTP Relay for the broadcast domain. When `disabled`, BOOTP Relay is performed by one of the global BOOTP servers. **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>* **vlan** *<VLAN number>* Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN. **Command mode:** Global configuration
no ip bootp-relay bcast-domain *<1-10>* Deletes the selected broadcast domain configuration. **Command mode:** Global configuration
show ip bootp-relay Displays the current parameters for the BOOTP Relay broadcast domain. **Command mode:** All

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. Lenovo N/OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the "High Availability" chapter in the *Lenovo N/OS 8.2 Application Guide.*

Table 319. *Virtual Router Redundancy Protocol Commands*

Command Syntax and Usage
`router vrrp` Enter Router VRRP configuration mode. **Command mode:** Global configuration
`[no] enable` Globally enables or disables VRRP on this switch. **Command mode:** Router VRRP
`group` Configures VRRP virtual routers groups. To view command options, see page 495. Command mode: Router VRRP
`holdoff` *<0-255>* Globally sets the time, in seconds, VRRP waits from when the master switch goes down until elevating a new switch to be the master switch. **Command mode:** Router VRRP
`[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
`interface` *<interface number>* Configures VRRP authentication parameters for the IP interfaces used with the virtual routers. To view command options, see page 498. **Command mode:** Router VRRP

Table 319. *Virtual Router Redundancy Protocol Commands*

Command Syntax and Usage
`tracking-priority-increment` Configures weights for the various criteria used to modify priority levels during the master router election process. To view command options, see page 499. **Command mode:** Router VRRP
`virtual-router` *<1-128>* Configures virtual routers for the switch. To view command options, see page 492. 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 320. *VRRP Virtual Router Configuration Commands*

Command Syntax and Usage
[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
[no] virtual-router *<1-128>* **enable** Enables or disables this virtual router. **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
[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). The default setting is `enabled`. **Command mode:** Router VRRP

Table 320. *VRRP Virtual Router Configuration Commands (continued)*

Command Syntax and Usage
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. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used, this base priority value can be modified according to a number of performance and operational criteria. The default value is **100**. **Command mode:** Router VRRP
virtual-router *<1-128>* **timers advertise** *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is **1**. **Command mode:** Router VRRP
virtual-router *<1-128>* **track** Enables the priority system used when electing the master router from a pool of virtual routers. To view command options, see page 494. **Command mode:** Router VRRP
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** *<128>* **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**. **Note:** All VRID values must be unique within the VLAN to which the virtual router's IP interface belongs. **Command mode:** Router VRRP
no virtual-router *<1-128>* Deletes this virtual router from the switch configuration. **Command mode:** Router VRRP
show ip vrrp virtual-router *<1-128>* Displays the current configuration information for this virtual router. **Command mode:** All

Virtual Router Priority Tracking Configuration

These commands are used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking commands.

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria apply to standard virtual routers, otherwise called "virtual interface routers." A virtual *server* router is defined as any virtual router whose IP address is the same as any configured virtual server IP address.

Table 321. *VRRP Priority Tracking Configuration Commands*

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

Virtual Router Group Configuration

Virtual Router Group commands are used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the 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 322. *VRRP Virtual Router Group Configuration Commands*

Command Syntax and Usage
`group advertisement` *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is `1`. **Command mode:** Router VRRP
`[no] group enable` Enables or disables the virtual router group. **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 preempt-delay-time` *<0-255>* Configures the preempt delay interval (in seconds). This timer is configured on the virtual router group and prevents the switch from transitioning back to Master state until the preempt delay interval has expired. Ensure that the interval is long enough for OSPF or other routing protocols to converge. The default is `0` seconds. **Command mode:** Router VRRP
`[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). The default setting is `enabled`. **Command mode:** Router VRRP

Table 322. *VRRP Virtual Router Group Configuration Commands (continued)*

Command Syntax and Usage
`group priority` *<1-254>* Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. 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. The default value is `100`. **Command mode:** Router VRRP
`group track` Enables the priority system used when electing the master router from a pool of virtual router groups. To view command options, see page 497. **Command mode:** Router VRRP
`group virtual-router-id` *<1-255>* Defines the virtual router ID (VRID). The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 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
`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 323. *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. The default setting is `disabled`. **Command mode:** Router VRRP
`[no] group track ports` When `enabled`, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. The default setting is `disabled`. **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 324. *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 494), the priority level for the virtual router is increased by a defined amount.

Table 325. *VRRP Tracking Configuration Commands*

Command Syntax and Usage
tracking-priority-increment interfaces *<0-254>* Defines the priority increment value for active IP interfaces detected on this switch. The default value is 2. **Command mode:** Router VRRP
tracking-priority-increment ports *<0-254>* Defines the priority increment value for active ports on the virtual router's VLAN. The default value is 2. **Command mode:** Router VRRP
tracking-priority-increment virtual-routers *<0-254>* Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2. **Command mode:** Router VRRP
show ip vrrp tracking-priority-increment Displays the current configuration of priority tracking increment values. **Command mode:** All

Note: These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Commands (see page 494) are enabled.

Protocol Independent Multicast Configuration

The following table displays Protocol Independent Multicast configuration commands:

Table 326. *PIM Configuration Options*

Command Syntax and Usage
ip pim component *<1-2>* Enter PIM component mode. See page 501 to view options. **Command mode**: Global configuration
[no] ip pim enable Globally enables or disables PIM. **Command mode**: Global configuration
[no] ip pim pmbr enable Enables or disables PIM border router. The default setting is `disabled`. **Command mode**: Global configuration
ip pim regstop-ratelimit-period *<0-2147483647>* Configures the register stop rate limit, in seconds. The default value is `5`. **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
clear ip pim mroute Clears PIM multicast router entries. **Command mode**: Global configuration

PIM Component Configuration

Use these commands to configure a PIM Component:

Table 327. *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 328. *RP Candidate Configuration Options*

Command Syntax and Usage
rp-candidate holdtime *<0-255>* Configures the hold time of the RP candidate, in seconds. **Command mode**: PIM Component
[no] rp-candidate rp-address *<group multicast address> <group subnet mask> <IP address>* Adds or removes an RP candidate. **Command mode**: PIM Component

RP Static Configuration

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

Table 329. *RP Static Configuration Options*

Command Syntax and Usage
[no] rp-static rp-address *<group multicast address> <group subnet mask> <IP address>* Adds or removes a static RP. **Command mode**: PIM Component

PIM Interface Configuration

The following table displays PIM Interface configuration commands:

Table 330. *PIM Interface Configuration Options*

Command Syntax and Usage
interface ip *<interface number>* Enter Interface IP mode. **Command mode**: Global Configuration
[no] ip pim border-bit Enables or disables the interface as a border router. The default setting is `disabled`. **Command mode**: Interface IP
[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 dr-priority *<0-4294967294>* Configures the designated router priority. The default value is `1`. **Command mode**: Interface IP
[no] ip pim enable Enables or disables PIM on the interface. **Command mode**: Interface IP
ip pim hello-interval *<0-65535>* Configures the time interval, in seconds, between PIM Hello packets. The default value is `30`. **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 join-prune-interval *<0-65535>* Configures the interval between Join Prune messages, in seconds. The default value is `60`. **Command mode**: Interface IP

Table 330. *PIM Interface Configuration Options (continued)*

Command Syntax and Usage
ip pim lan-delay *<0-32767>* Configures the LAN delay value for the router interface, in seconds. **Command mode**: Interface IP
[no] ip pim lan-prune-delay Enables or disables LAN delay advertisements on the interface. The default setting is `disabled`. **Command mode**: Interface IP
ip pim neighbor-addr *<IP address>* **{allow|deny}** Allows or denies PIM access to the specified neighbor. You can configure a list of up to 72 neighbors that bypass the neighbor filter. Once you configure the interface to allow a neighbor, you can configure the interface to deny the neighbor. **Command mode**: Interface IP
[no] ip pim neighbor-filter Enables or disables the PIM neighbor filter on the interface. When `enabled`, this interface does not accept any PIM neighbors, unless specifically permitted using the following command: `ip pim neighbor-addr` *<IP address>* **Command mode**: Interface IP
ip pim override-interval *<0-65535>* Configures the override interval for the router interface, in seconds. **Command mode**: Interface IP
show ip pim interface [*<interface number>***|detail]** Displays the current PIM interface parameters. **Command mode**: All
show ip pim neighbor-filters Displays the configured PIM neighbor filters. **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 used for management traffic.

Table 331 describes the IPv6 Default Gateway Configuration commands.

Table 331. *IPv6 Default Gateway Configuration Commands*

Command Syntax and Usage
ip gateway6 *<1,3-4>* **address** *<IPv6 address>* **[enable]** Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as `3001:0:0:0:0:0:abcd:12`). The `enable` option also enable the default gateway. **Command mode**: Global configuration
[no] ip gateway6 *<1,3-4>* **enable** Enables or disables the default gateway. **Command mode**: Global configuration
no ip gateway6 *<1,3-4>* Deletes the default gateway. **Command mode**: Global configuration
show ipv6 gateway6 *<1,3-4>* Displays the current IPv6 default gateway configuration. **Command mode**: All

IPv6 Static Route Configuration

Table 332 describes the IPv6 static route configuration commands.

Table 332. *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
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: o `destination-address`: Destination IPv6 address of the route o `gateway`: Default gateway address used by the route o `interface`: Interface used by the route o `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 333 describes the IPv6 Neighbor Discovery cache configuration commands.

Table 333. *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>***|interface port** *<port alias or number>***|vlan** *<VLAN number>***]** Clears the selected static entries in the Neighbor Discovery cache table. **Command mode**: Global configuration

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 334. *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 in this table. **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 334. *IPv6 Neighbor Discovery Prefix Commands (continued)*

Command Syntax and Usage
ipv6 nd prefix {<*IPv6 prefix*> <*prefix length*>**} no-autoconfig** Disables the autonomous flag. When `enabled`, the autonomous flag indicates that the prefix can be used for stateless address configuration. The default setting is `enabled`. **Command mode**: Interface IP
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*>**}** **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
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 335. *IPv6 Prefix Policy Table Options*

Command Syntax and Usage
`[no] ip prefix-policy` *<IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)>* Adds or removes a Prefix Policy Table entry. Enter the following parameters: o `IPv6 address prefix` o `Prefix length` o `Precedence`: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence. o `Label`: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match. **Command mode**: Global configuration
`show ip prefix-policy` Displays the current Prefix Policy Table configuration. **Command mode**: All

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 336. *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`. **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

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 337. *IP Loopback Interface Commands*

Command Syntax and Usage
`interface loopback` *<1-5>* Enter Interface Loopback mode. **Command mode**: Global configuration
`[no] enable` Enables or disables the loopback interface. **Command mode**: Interface loopback
`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
`no interface loopback` *<1-5>* Deletes the selected loopback interface. **Command mode**: Global configuration
`show interface loopback` *<1-5>* Displays the current IP loopback interface parameters. **Command mode**: All

Converged Enhanced Ethernet Configuration

Table 338 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 338. *CEE Commands*

Command Syntax and Usage
`[no] cee enable` Globally enables or disables CEE. **Command mode**: Global configuration
`[no] cee iscsi enable` Enables or disables ISCSI TLV advertisements. **Command mode**: Global configuration
`show cee` Displays the current CEE parameters. **Command mode**: All
`show cee iscsi` Displays the current ISCSI TLV 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 339 describes the global ETS Priority Group configuration options.

Table 339. *Global ETS Priority Group Commands*

Command Syntax and Usage
[no] cee global ets mcast-priority-group mcpgid *<0-3>* **[bandwidth percentage** *<0, 10-100>***] [priority** *<0-7>***]** Configures Multicast Priority Group parameters. You can enter the link bandwidth percentage allocated to the Multicast Priority Group, and assign one or more 802.1p values to the Multicast Priority Group. **Command mode**: Global configuration
cee global ets mcast-priority-group mcpgid *<0-3>* **description** *<1-31 characters>* Enter text that describes the multicast priority group. **Command mode**: Global configuration
no cee global ets mcast-priority-group mcpgid *<0-3>* **description** Removes the description for the specified multicast priority group. **Command mode**: Global configuration
cee global ets priority-group pgid *<0-7, 15>* **bandwidth** *<802.1p priority (0-7)> <bandwidth percentage (0, 10-100)>* Allows you to configure Priority Group parameters. You can enter the link bandwidth percentage allocated to the Priority Group, and also assign one or more 802.1p values to the Priority Group. **Command mode**: Global configuration
cee global ets priority-group pgid *<0-7, 15>* **description** *<1-31 characters>* Enter text that describes this Priority Group. **Command mode**: Global configuration
no cee global ets priority-group *<0-7, 15>* **description** Removes the description for the specified Priority Group. **Command mode**: Global configuration

Table 339. *Global ETS Priority Group Commands*

Command Syntax and Usage
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 Displays the current global ETS Priority Group parameters. **Command mode**: All
show cee global ets mcast-priority-group *<0-3>* Displays the current global ETS Multicast Priority Group parameters. **Command mode**: All
show cee global ets priority-group *<0-7, 15>* Displays the current global ETS Priority Group parameters. **Command mode**: All

Priority Flow Control Configuration

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

Global Priority Flow Control Configuration

Table 340 describes the global PFC Priority Group configuration options.

Table 340. *Global PFC Prority Group Commands*

Command Syntax and Usage
[no] cee global pfc enable Globally enables or disables Priority Flow Control on all ports. **Command mode:** Global configuration
cee global pfc priority *<0-7>* **description** *<1-31 characters>* Enter text that describes this Priority Group. **Command mode:** Global configuration
no cee global pfc priority *<0-7>* **description** Removes the description for the specified Priority Group. **Command mode:** Global configuration
[no] cee global pfc priority *<0-7>* **enable** Enables or disables Priority Flow Control for the specified priority level. **Command mode:** Global configuration
show cee global pfc Displays the current Priority Flow Control global configuration. **Command mode:** All

Port-level 802.1p PFC Configuration

Table 341 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 341. *Port 802.1p PFC Options*

Command Syntax and Usage
[no] cee port *<port alias or number>* **pfc enable** Enables or disables Priority Flow Control on the selected port. **Command mode**: Global configuration
cee port *<port alias or number>* **pfc priority** *<0-7>* **description** *<1-31 characters>* Enter text to describe the priority value. **Command mode**: Global configuration
no cee port *<port alias or number>* **pfc priority** *<0-7>* **description** Deletes the description from the specified priority value. **Command mode:** Global configuration
[no] cee port *<port alias or number>* **pfc priority** *<0-7>* **enable** Enables or disables Priority Flow Control on the selected 802.1p priority. **Note**: PFC can be enabled on 802.1p priority 3 and one other priority only. **Command mode**: Global configuration
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 342 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 342. *Port DCBX Commands*

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

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 348 describes generic Fibre Channel configuration options.

Table 343. *Fibre Channel Configuration Commands*

Command Syntax and Usage
`[no] system port` *<port number or range>* **`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> <VLAN number>* Configures or removes an FC alias name for the specified port World Wide Name. **Command mode:** Global configuration
`fcdomain domain` *<0-239>* **`{preferred|static}`** *<VLAN number>* Configures the domain type for the specified FC domain ID: o `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. o `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` *<VLAN number>* Erases all FC zones and zonesets. **Command mode:** Global configuration

FC Port Configuration

Use the following commands to configure Fibre Channel ports.

Table 344. *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
shutdown Disables the FC port. The default setting is enabled (`no shutdown`). **Command mode:** FC Port configuration
no shutdown Enables the FC port. The default setting is enabled (`no shutdown`). **Command mode:** FC Port configuration
fc-speed {*4***|***8***|auto}** Configures the Fibre Channel port speed in Gbps or allows the port to negotiate its speed automatically. The default setting is `auto`. **Command mode:** FC Port configuration
[no] type e Enable the FC port to type E or disable the E port. **Command mode**: FC Port configuration

FC VLAN Configuration

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

Table 345. *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. The default setting is `disabled`. **Command mode:** VLAN configuration

Table 345. *FCF VLAN Configuration Commands*

Command Syntax and Usage
`npv disruptive-load-balance` Triggers a disruptive load-balance among the logged-in nodes in the current NPV VLAN. **Command mode:** VLAN configuration
`[no] npv enable` Enables or disables NPV gateway functionality for the VLAN. The default setting is `disabled`. **Command mode:** VLAN configuration
`[no] npv traffic-map external-interface` *<port numbers or range>* 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
`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 346. *Fibre Channel Zone Configuration Commands*

Command Syntax and Usage
[no] zone name *<1-64 characters> <VLAN number>* 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> <VLAN number>* Creates a new zone with the attributes of the selected zone. **Command mode:** Global configuration
zone rename *<current_name> <new_name> <VLAN number>* Renames the FC zone. **Command mode:** Global configuration
[no] zone default-zone permit *<VLAN number>* 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: o pwwn: Port World Wide Number o fcid: FC ID of the port, in hex format (for example, 0xce00d1). o 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 347. *Fibre Channel Zoneset Configuration Commands*

Command Syntax and Usage
[no] zoneset name *<1-64 characters> <VLAN number>* 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> <VLAN number>* 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> <VLAN number>* Creates a new zoneset with the attributes of the selected zoneset. **Command mode:** Global configuration
zone copy active-zoneset running-config *<VLAN number>* Copies the active zoneset database to the running configuration. **Command mode:** Global configuration
zoneset rename *<current_name> <new_name> <VLAN number>* 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 348 describes the FCoE configuration options.

Table 348. *FCoE Configuration Commands*

Command Syntax and Usage
`[no] fcoe fips enable` Globally enables or disables FIP Snooping on. **Command mode**: Global configuration
`[no] fcoe fips timeout-acl` Enables or disables ACL time-out removal. When `enabled`, ACLs associated with expired FCFs and FCoE connections are removed from the system. **Command mode**: Global configuration
`[no] fcoe optimized-forwarding enable` Enables or disables QLogic Fibre Channel optimized forwarding. The default value is `enabled`. **Command mode**: Global configuration
`show fcoe information` Displays the current FCoE parameters. **Command mode**: All
`show fcoe optimized-acl vlan` *<1-4095>* Displays optimized ACLs used for a specific VLAN. **Command mode**: All
`show fcoe optimized-forwarding status` Displays whether QLogic Fibre Channel optimized forwarding is enabled or not. **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 349 describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 349. *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: o `on`: Configures the port as a Fibre Channel Forwarding (FCF) port. o `off`: Configures the port as an FCoE node (ENode). o `auto`: Automatically detect the configuration of the connected device, and configure this port to match. **Command mode**: Global configuration
`[no] fcoe fips port` *<port alias or number>* **`enable`** Enables or disables 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

Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

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

RMON History Configuration

Table 350 describes the RMON History commands.

Table 350. *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>* **`owner`** *<1-127 characters>* Enter a text string that identifies the person or entity that uses this History index. **Command mode**: Global configuration
`rmon history` *<1-65535>* **`polling-interval`** *<1-3600>* Configures the time interval over which the data is sampled for each bucket. The default value is `1800`. **Command mode**: Global configuration
`rmon history` *<1-65535>* **`requested-buckets`** *<1-65535>* Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is `30`. **Note:** The maximum number of buckets that can be granted is 50. **Command mode**: Global configuration

Table 350. *RMON History Commands (continued)*

Command Syntax and Usage
no rmon history *<1-65535>* Deletes the selected History index. **Command mode**: Global configuration
show rmon history Displays the current RMON History parameters. **Command mode**: All

RMON Event Configuration

Table 351 describes the RMON Event commands.

Table 351. *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
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>* **type {log|trap|both}** Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station. **Command mode**: Global configuration
no rmon event *<1-65535>* 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 352 describes the RMON Alarm commands.

Table 352. *RMON Alarm Commands*

Command Syntax and Usage
rmon alarm *<1-65535>* **alarm-type {rising|falling|either}** Configures the alarm type as rising, falling, or either (rising or falling). **Command mode**: Global configuration
rmon alarm *<1-65535>* **falling-crossing-index** *<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>* **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>* **interval** *<1-65535>* Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is **1800**. **Command mode**: Global configuration
rmon alarm *<1-65535>* **oid** *<1-127 characters>* Configures an alarm MIB Object Identifier. **Command mode**: Global configuration
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
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

Table 352. *RMON Alarm Commands (continued)*

Command Syntax and Usage
rmon alarm *<1-65535>* **rising-limit** *<-2147483647 - 2147483647>* Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. **Command mode**: Global configuration
rmon alarm *<1-65535>* **sample {abs|delta}** Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: o `abs`—absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. o `delta`—delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds. **Command mode**: Global configuration
no rmon alarm *<1-65535>* Deletes the selected RMON Alarm index. **Command mode**: Global configuration
show rmon alarm Displays the current RMON Alarm parameters. **Command mode**: All

Virtualization Configuration

Table 353 describes the VMReady configuration options.

Table 353. *VMReady Configuration Options*

Command Syntax and Usage
[no] virt enable Enables or disables VMReady. **Note**: The no form of this command deletes all configured VM groups. **Command mode**: Global configuration
virt evb profile Configures Edge Virtual Bridging (EVB) Virtual Station Interface Type profile settings. For command options, see page 546. **Command mode:** Global configuration
virt evb vsidb Configures Edge Virtual Bridging (EVB) VSI Type Database settings. For command options, see page 544. **Command mode:** Global configuration
virt vmcheck Configures VM Check validation settings. For command options, see page 537. **Command mode:** Global configuration
virt vmgroup Configures VM Group settings. For command options, see page 534. **Command mode:** Global configuration
virt vmpolicy vmbwidth Configures VM Bandwidth management settings. For command options, see page 530. **Command mode:** Global configuration
virt vmprofile Configures VM Profile settings. For command options, see page 538. **Command mode:** Global configuration
virt vmrmisc Configures Miscellaneous VMready settings. For command options, see page 540. **Command mode:** Global configuration

Table 353. *VMReady Configuration Options*

Command Syntax and Usage
`virt vmware` Configures VMware settings. For command options, see page 539. **Command mode:** Global configuration
`show virt` Displays the current virtualization parameters. **Command mode**: All

VM Policy Bandwidth Management

Table 354 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 354. *VM Bandwidth Management Options*

Command Syntax and Usage
[no] virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**] bwctrl** Enables or disables bandwidth control on the VM policy. **Command mode**: Global configuration
virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**] rxrate** <*0-40000000*> <*max. burst (0-4096)*> The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096. **Command mode:** Global configuration
virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**] txrate** <*0-40000000*> <*max. burst (0-4096)*> **[**<*ACL number (1-256)*>**]** The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096. The third 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
no virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**]** Deletes the bandwidth management settings from this VM policy. **Command mode**: Global configuration
show virt vmpolicy vmbwidth [<*MAC address*>**|**<*UUID*>**|**<*name*>**|** **|**<*IP address*>**|**<*index number*>**]** Displays the current VM bandwidth management parameters. **Command mode**: All

Virtual NIC Configuration

Table 355 describes the Virtual NIC (vNIC) configuration options.

Table 355. *Virtual NIC options*

Command Syntax and Usage
`[no] vnic egress-bw-meter` Enables or disables vNIC bandwidth metering. When enabled, any bandwidth which is not used by the vNIC to which it is allocated is shared with other vNICs. In all cases, the configured values for minimum bandwidth are honored. Only the excess bandwidth is shared. **Command mode**: Global configuration
`[no] vnic enable` Globally enables or disables vNIC. **Command mode**: Global configuration
`[no] vnic uplink-share` Enable or disable vNIC shared mode. When enabled, multiple vNIC groups can be assigned to the same uplink port. **Command mode**: Global configuration
`show vnic` Displays the current vNIC parameters. **Command mode**: All

vNIC Port Configuration

Table 356 describes the Virtual NIC (vNIC) port configuration options.

Table 356. *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
`[no] enable` Enables or disables the vNIC. **Command mode**: vNIC configuration

Virtual NIC Group Configuration

Table 357 describes the Virtual NIC (vNIC) Group configuration options.

Table 357. *vNIC Group Commands*

Command Syntax and Usage
vnic vnicgroup *<1-32>* Enters vNIC Group Configuration mode. **Command mode:** Global Configuration
[no] enable Enables or disables 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 all vNIC and non-vNIC ports in the group. Other port functions continue to operate normally. The default setting is `disabled`. **Command mode:** vNIC Group configuration
[no] key *<trunk number>* Adds or removes the uplink LACP trunk to the vNIC Group. **Command mode:** vNIC Group configuration
[no] member *<vNIC number>* Adds or removes a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: `1.1.` **Command mode:** vNIC Group configuration
[no] port *<port number or alias>* Adds or removes the non-vNIC port or uplink port to the vNIC Group. **Command mode:** vNIC Group configuration
[no] trunk *<trunk number>* Adds or removes the uplink trunk group to the vNIC Group. **Command mode:** vNIC Group configuration
no trunk *<trunk number>* Removes the uplink trunk group from the vNIC Group. **Command mode:** vNIC Group configuration
vlan *<VLAN number>* Assigns a VLAN to the vNIC Group. **Command mode:** vNIC Group configuration

Table 357. *vNIC Group Commands (continued)*

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

VM Group Configuration

Table 358 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 358. *VM Group Commands*

Command Syntax and Usage
virt vmgroup *<1-4096>* **cpu** Enables or disables sending unregistered IPMC traffic to CPU. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **flood** Enables or disables flooding unregistered IPMC traffic. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **key** *<1-65535>* Adds or removes 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
virt vmgroup *<1-4096>* **optflood** Enables or disables optimized flooding. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **port** *<port number or alias>* Adds or removes the selected port to the VM group. **Note**: A port can be added to a VM group only if no VMs on that port are members of the VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **portchannel** *<trunk number>* Adds or removes the selected trunk group to the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **profile** *<profile name (1-39 characters)>* Adds the selected VM profile to the VM group. **Command mode:** Global configuration
no virt vmgroup *<1-4096>* **profile** Removes the VM profile assigned to the VM group. **Note:** This command can only be used if the VM group is empty (only has the profile assigned). **Command mode:** Global configuration

Table 358. *VM Group Commands (continued)*

Command Syntax and Usage
virt vmgroup *<1-4096>* **stg** *<STG number>* Assigns the VM group VLAN to a Spanning Tree Group (STG). **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **tag** Enables or disables VLAN tagging on ports in this VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **validate [basic|advanced]** Enables MAC address spoof prevention for the specified VM group. Default setting is disabled. o `basic` validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for "trusted" hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines. o `advanced` validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for "untrusted" hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines. **Command mode:** Global configuration
no virt vmgroup *<1-4096>* **validate** Disables MAC address spoof prevention for the specified VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **vm [**<*MAC address*>**|**<*UUID*>**|**<*name*>**|** <*IP address*>**|**<*index number*>**]** Adds or removes a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (`virt vmware vcspec`). The VM index number is found in the VM information dump (`show virt vm`). **Note**: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group. **Command mode:** Global configuration
[no] virt vmgroup *<1-4096>* **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 361. **Command mode:** Global configuration

Table 358. *VM Group Commands (continued)*

Command Syntax and Usage
[no] virt vmgroup *<1-4096>* **vport** *<virtual port alias or number>* Adds or removes the selected virtual port to the VM group. **Command mode:** Global configuration
virt vmgroup *<1-4096>* **vlan** *<VLAN number>* Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns 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 *<1-4096>* Deletes the VM group. **Command mode:** Global configuration
show virt vmgroup *<1-4096>* Displays the current VM group parameters. **Command mode:** All

VM Check Configuration

Table 359 describes the VM Check validation options used for MAC address spoof prevention.

Table 359. *VM Check Configuration Options*

Command Syntax and Usage
`virt vmcheck acls max` *<1-256>* Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. The default value is `50`. **Command mode:** Global configuration
`no virt vmcheck acls` Disables ACL-based MAC address spoofing prevention in advanced validation mode. **Command mode:** Global configuration
`virt vmcheck action advanced {acl|link|log}` Sets up action taken when detecting MAC address spoofing in advanced validation mode: o `acl` registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address o `link` registers a syslog entry and disables the corresponding switch port o `log` registers a syslog entry The default setting is `acl`. **Command mode:** Global configuration
`virt vmcheck action basic {link|log}` Sets up action taken when detecting MAC address spoofing in basic validation mode: o `link` registers a syslog entry and disables the corresponding switch port o `log` registers a syslog entry The default setting is `link`. **Command mode:** Global configuration
`[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 149 for sample output. **Command mode:** Global configuration

VM Profile Configuration

Table 360 describes the VM Profiles configuration options.

Table 360. *VM Profiles Commands*

Command Syntax and Usage
virt vmprofile *<profile name (1-39 characters)>* Defines a name for the VM profile. **Command mode:** Global configuration
no virt vmprofile *<profile name (1-39 characters)>* Deletes the selected VM profile. **Command mode:** Global configuration
[no] virt vmprofile edit *<profile name (1-39 characters)>* **eshaping [***<average (1-1000000000)>* *<burst (1-1000000000)>* *<peak (1-1000000000)>***]** Configures traffic egress shaping parameters implemented in the hypervisor, as follows: o Average traffic, in Kilobits per second o Maximum burst size, in Kilobytes o Peak traffic, in Kilobits per second o Delete traffic shaping parameters. **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: o Average traffic, in Kilobits per second o Maximum burst size, in Kilobytes o Peak traffic, in Kilobits per second o Delete traffic shaping parameters. **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
show virt vmprofile [*<profile name>***]** Displays the current VM Profile parameters. **Command mode:** All

VMWare Configuration

Table 361 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.

Note: VM Profiles and Hello cannot be configured or enabled unless the Virtual Center is configured.

Table 361. *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
`virt vmware hello [enable|haddr` *<IP_address>***`|`** **`|hport`** *<port_no>***`|htimer`** *<1-60>***`]`** Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention. Default setting is `disabled`. o `enable` enables CDP advertisements transmission. o `haddr` advertises a specific IP address instead of the default management IP. o `hport` enables ports on which CDP advertisements are sent. o `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
`[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

Table 361. *VM Ware Commands*

Command Syntax and Usage
`show virt vmware` Displays the current VMware parameters. **Command mode:** All

Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the Lenovo N/OS CLI, ISCLI and the Miscellaneous VMready Configuration Menu. Table 361 describes the VMready configuration options.

Table 362. *VMware Miscellaneous Options*

Command Syntax and Usage
`[no] virt vmrmisc lmac` Enables or disables the switch to treat locally administered MAC addresses as VMs. **Command mode**: Global configuration
`[no] virt vmrmisc oui` *< 3 byte VM MAC OUI> <Vendor Name>* Adds or removes a MAC OUI. **Command mode**: Global configuration
`show virt oui` Displays all the configured MAC OUIs. **Command mode**: All

UFP Configuration

Table 363 describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 4 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, FCoE, auto) and within predefined bandwidth limits.

Note: vNIC and UFP are mutually exclusive. Only one of them can be globally enabled at any point in time.

Table 363. *UFP Commands*

Command Syntax and Usage
[no] ufp enable Globally enables or disables UFP. **Command mode:** Global configuration
[no] ufp port *<port_no.>* **enable** Enables or disables UFP on the specified physical ports. **Command mode:** Global configuration
ufp port *<port_no.>* **vport** *<1-4>* Enters UFP Virtual Port Configuration mode. **Command mode:** Global configuration
no ufp port *<port_no.>* **[vport** *<1-4>***]** Disables UFP settings on the specified physical or virtual port. **Command mode:** Global configuration
[no] enable Enables or disables the virtual port. **Command mode:** UFP Virtual Port Configuration
evb profile *<1-16>* Applies the specified EVB profile for the virtual port. **Command mode:** UFP Virtual Port Configuration
no evb profile Disables the specified EVB profile for the virtual port. **Command mode:** UFP Virtual Port Configuration

Table 363. *UFP Commands (continued)*

Command Syntax and Usage
network {default-tag|default-vlan *<2-4094>***}** Configures the virtual port network configuration settings: o `default-tag` enables tagging egress frames with the default VLAN ID when the virtual port is in access or trunk mode and `default-vlan` is defined. Default setting is `disabled`. o `default-vlan` configures the default VLAN ID for the virtual port. **Note:** VLANs 4002-4005 cannot be used as customer VLANs. **Note:** A customer VLAN cannot be configured on multiple virtual ports of the same physical port. **Command mode:** UFP Virtual Port Configuration
no network default-tag Disables default VLAN ID tagging on the virtual port. **Command mode:** UFP Virtual Port Configuration
network mode {access|auto|fcoe|trunk|tunnel} Configures the virtual port's operating mode: o `access` allows the virtual port to associate only with the default customer VLAN, as defined by the `network default-vlan` command. o `auto` integrates UFP with VMReady/802.1qbg. This mode allows dynamic vlan creation for the vport. o `fcoe` configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. Setting a virtual port in `fcoe` mode enables Priority Flow Control on the physical port. o `trunk` allows the virtual port to associate with up to 1024 customer VLANs. o `tunnel` makes the virtual port VLAN agnostic. This is the default setting. **Command mode:** UFP Virtual Port Configuration
network private-vlan {host|trunk} Configures the virtual port's private VLAN mode : o `host` allows only ONE secondary VLAN. In case of network trunk mode, the other VLANs will be in different Private VLAN domain. o `trunk` allows both primary and secondary VLAN as well as non-Private VLAN domains. The Isolate-VLAN is also allowed to pass through this port type. **Command mode:** UFP Virtual Port Configuration

Table 363. *UFP Commands (continued)*

Command Syntax and Usage
no network private-vlan Disables private-VLAN mode on the virtual port. **Command mode:** UFP Virtual Port Configuration
qos bandwidth {max *<10-100>***|min** *<10-100>***}** Configures bandwidth allocation for the virtual port: o Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is 25. o Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is 100. **Note**: The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100. **Command mode:** UFP Virtual Port Configuration

Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). Table 364 describes the EVB configuration options.

Table 364. *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
filename *<file name>* Sets the Virtual Station Interface Type database document name. **Command mode:** VSI Database
no filename Removes the Virtual Station Interface Type database document name. **Command mode:** VSI Database
filepath *<file path>* Sets the Virtual Station Interface Type database document path. **Command mode:** VSI Database
no filepath Removes the Virtual Station Interface Type database document path. **Command mode:** VSI Database
host *<IP address>* **[mgt-port|extm-port|data-port]** Sets the Virtual Station Interface Type database manager IPv4/IPv6 address and the port used for the connection. By default, the management port is used. **Command mode:** VSI Database
port *<1-65534>* Sets the Virtual Station Interface Type database manager port. **Command mode:** VSI Database
protocol {http|https} Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP. **Command mode:** VSI Database

Table 364. *Edge Virtual Bridge Configuration Options*

Command Syntax and Usage
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
no virt evb vsidb *<VSIDB_number>* Resets the Virtual Station Interface Type database information to the default values. **Command mode:** Global configuration
clear virt evb vsi [mac-address|port *<port alias or number>***|** **|type-id** *<1-16777215>***|vlan** *<1-4094>***]** Clears VSI database associations. **Command mode**: All
clear virt evb vsidb [manager-id *<0-255>***|type-id** *<1-16777215>***|** **|version** *<0-255>***]** Clears local VSI types cache. **Command mode**: All
show virt evb vsitypes [mgrid *<0-255>***|typeid** *<1-16777215>***|** **|version** *<0-255>***]** Displays the current Virtual Station Interface Type database parameters. **Command mode:** All
show virt evb vsidb *<VSIDB_number>* Displays the current Virtual Station Interface database information. **Command mode:** All

Edge Virtual Bridge Profile Configuration

Table 365 describes the Edge Virtual Bridge profile configuration options.

Table 365. *Edge Virtual Bridge VSI Type Profile Configuration Options*

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

Switch Partition (SPAR) Configuration

Switch partitions (SPARs) divide the data plane inside a physical switch into independent switching domains. Switch partitions do not communicate with each other, forcing hosts on different SPARs to bridge traffic over an upstream link, even if they belong to the same VLAN.

Up to 8 SPARs can be defined on a switch. Each SPAR supports up to 32 local VLANs, for further partitioning flexibility.

Table 366. *SPAR Configuration Options*

Command Syntax and Usage
spar *<1-8>* Enters SPAR Configuration mode. **Command mode:** Global configuration
no spar *<1-8>* Deletes the specified SPAR. **Command mode:** Global configuration
[no] enable Enables or disables the SPAR. **Command mode:** SPAR Configuration
name Configures the SPAR name. **Command mode:** SPAR Configuration
domain default {vlan *<2-4094>***|member** *<port no.>***}** Configures the SPAR's default domain settings: o `vlan` configures the default SPAR VLAN ID. A unique factory default VLAN ID is assigned to each SPAR as "408x", where x is the SPAR ID *<1-8>*. This option provides an override if conflicts arise with a customer VLAN ID on the upstream network. o `member` adds server ports to the SPAR. **Command mode:** SPAR Configuration
no domain default member *<port no.>* Removes server ports from the SPAR. **Command mode:** SPAR Configuration

Table 366. *SPAR Configuration Options (continued)*

Command Syntax and Usage
domain local *<1-32>* **{enable|member** *<port no.>***|name** *<text>***| |vlan** *<2-4094>***}** Configures the SPAR's local domains: o `enable` enables the SPAR local domains o `member` adds server ports to the SPAR local domains o `name` configures the SPAR local domains names o `vlan` applies a VLAN ID to the SPAR local domains. The default value is 0. **Command mode:** SPAR Configuration
no domain local *<1-32>* **[enable|member** *<port no.>* **|vlan]** Deletes the SPAR local VLAN domains: o `enable` disables the SPAR local domains o `member` deletes SPAR local domains server ports o `vlan` deletes SPAR local domains vlan. **Command mode:** SPAR Configuration
domain mode {passthrough|local} Configures the SPAR domain mode: o `passthrough` references member ports only by the SPAR default VLAN. This provides VLAN-unaware uplink connectivity via pass-through tunnel domain switching for SPAR member ports. The default value is `passthrough`. o `local` references member ports by both SPAR default VLAN and SPAR local domain VLANs. This provides VLAN-aware uplink connectivity via local domain switching for SPAR member ports **Command mode:** SPAR Configuration
[no] uplink {port *<port no.>***|portchannel** *<1-64>***|adminkey** *<1-65535>***}** Enables or disables uplink connectivity for the SPAR. A single external port, portchannel, or LACP channel can be used for uplink. All uplinks within a SPAR are automatically assigned to the SPAR domain's default VLAN and to any SPAR local VLANs. **Command mode:** SPAR Configuration
show spar *<1-8>* **[domain [default|local** *<1-32>***]|uplink]** Displays the SPAR settings: o `domain` filters only the SPAR domain related settings • `default` filters only SPAR default domain settings • `local` *<1-32>* filters only SPAR local domains settings o `uplink` filters only SPAR uplink settings **Command mode:** All

Service Location Protocol Configuration

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

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

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

Table 367. *Service Location Protocol Options*

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

Configuration Dump

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

```
CN 4093(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, as described on page 552.

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:

```
CN 4093(config)# copy running-config ftp [data-port|extm-port|mgt-port]
```

or:

```
CN 4093(config)# copy running-config tftp [data-port|extm-port|mgt-port]
```

or:

```
CN 4093(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:

```
CN 4093(config)# copy ftp running-config [data-port|extm-port|mgt-port]
```

or:

```
CN 4093(config)# copy tftp running-config [data-port|extm-port|mgt-port]
```

or:

```
CN 4093(config)# copy sftp running-config [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.

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 368. *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 369. *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
[no] interface portchannel *<1-128>* **shutdown** Temporarily enables or disables the specified port channel. The port channel will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
[no] interface portchannel lacp *<1-65535>* **shutdown** Temporarily enables or disables specified LACP trunk groups. **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 370. *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: o `force unauth`: the port is placed in unauthorized state, and traffic is blocked. o `auto`: the port is placed in unauthorized state, then authentication is initiated. o `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 VRRP Commands

The following table displays Virtual Router Redundancy operations commands.

Table 371. *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: o This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same) o This switch's virtual router has a higher priority and preemption is enabled. o There are no other virtual routers available to take master control. **Command Mode**: Privileged EXEC

Operations-Level BGP Commands

The following table displays IP BGP operations commands.

Table 372. *IP BGP Operations Commands*

Command Syntax and Usage
router bgp start *<1-12>* Starts the peer session. **Command Mode**: Privileged EXEC
router bgp stop *<1-12>* 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 373. *Protected Mode Options*

Command Syntax and Usage
[no] protected-mode enable Enables or disables Protected Mode. When Protected Mode is `enabled`, the switch takes exclusive local control of all enabled options. When Protected Mode is `disabled`, the switch relinquishes exclusive local control of all enabled options. **Command Mode**: Global Configuration
[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 373. *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
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 374. *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: o Port Group name o VMware host ID (Use host UUID, host IP address, or host name.) o Virtual Switch name o VLAN ID of the Port Group o Whether to enable the traffic-shaping profile (`1` or `0`). If you choose `1` (yes), you are prompted to enter the traffic shaping parameters. **Command Mode**: All
`no virt vmware pg` *<Port Group name> <host ID>* Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All
`[no] virt vmware vsw` *<host ID> <Virtual Switch name>* Adds or removes a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All

Table 374. *VMware Operations Commands (continued)*

Command Syntax and Usage
virt vmware export *<VM profile name> <VMware host ID> <Virtual Switch name>* Exports a VM Profile to a VMware host. Use one of the following identifiers to specify each host: o UUID o IP address o Host name You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch. **Command Mode**: All
virt vmware scan Performs a scan of the VM Agent, and updates VM information. **Command Mode**: All
virt vmware vmacpg *<MAC address> <Port Group name>* Changes a VM NIC's configured Port Group. **Command Mode**: All
virt vmware updpg *<Port Group name> <host ID> <VLAN number>* **[***<shaping enabled> <average Kbps> <burst KB> <peak Kbps>***]** Updates a VMware host's Port Group parameters. **Command Mode**: All

VMware Distributed Virtual Switch Operations

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

Table 375. *VMware dvSwitch Operations (/oper/virt/vmware/dvswitch)*

Command Syntax and Usage
virt vmware dvswitch add *<datacenter name> <dvSwitch name> <dvSwitch version>* Adds the specified dvSwitch to the specified DataCenter. **Command Mode**: All
virt vmware dvswitch del *<datacenter name> <dvSwitch name>* Removes the specified dvSwitch from the specified DataCenter. **Command Mode**: All
virt vmware dvswitch addhost *<dvSwitch name>* **{***<host UUID>***|** **|***IP address***|***host name***>}** Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode**: All
virt vmware dvswitch remhost *<dvSwitch name>* **{***<host UUID>***|** **|***IP address***|***host name***>}** Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host: o UUID o IP address o Host name **Command Mode:** All
virt vmware dvswitch addUplink *<dvSwitch name> <host ID> <uplink name>* Adds the specified physical NIC to the specified dvSwitch uplink ports. **Command Mode**: All
virt vmware dvswitch remUplink *<dvSwitch name> <host ID> <uplink name>* Removes the specified physical NIC from the specified dvSwitch uplink ports. **Command Mode**: All

VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

Table 376. *VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)*

Command Syntax and Usage
virt vmware dpg add *<port group name> <dvSwitch name> <VLAN ID>* **[ishaping** *<bandwidth> <burst size> <peak bandwidth>***]** **[eshaping** *<bandwidth> <burst size> <peak bandwidth>***]** Adds the specified port group to the specified dvSwitch. You may enter the following parameters: o `ishaping`: Enables ingress shaping. Supply the following information: • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second o `eshaping`: Enables engress shaping. Supply the following information: • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second **Command Mode**: All
virt vmware dpg vmac *<VNIC MAC> <port group name>* Adds the specified VM NIC to the specified port group. **Command Mode**: All
virt vmware dpg update *<port group name> <dvSwitch name> <VLAN ID>* **[ishaping** *<bandwidth> <burst size> <peak bandwidth>***]** **[eshaping** *<bandwidth> <burst size> <peak bandwidth>***]** Updates the specified port group on the specified dvSwitch. You may enter the following parameters: o `ishaping`: Enables ingress shaping. Supply the following information: • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second o `eshaping`: Enables engress shaping. Supply the following information: • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second **Command Mode**: All
virt vmware dpg del *<port group name> <dvSwitch name>* Removes the specified port group from the specified dvSwitch. **Command Mode**: All

Edge Virtual Bridge Operations

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

Table 377. *Edge Virtual Bridge Operations Commands*

Command Syntax and Usage
virt evb update vsidb *<VSIDB_number>* Update VSI types from the VSI database. **Command mode**: All
clear virt evb vsidb [mgrid *<0-255>***|typeid** *<1-16777215>***|** **|version** *<0-255>***]** Clears local VSI types cache. **Command mode**: Privileged EXEC
clear virt evb vsi [mac-address|port *<port alias or number>***|** **|type-id** *<1-16777215>***|vlan** *<1-4094>***]** Clears VSI database associations. **Command mode**: Privileged EXEC

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 378. *Feature on Demand Key Options*

Command Syntax and Usage
`software-key` Enter FOD Key mode. **Command mode:** Privileged EXEC
`enakey address` *<hostname or IP address>* **`keyfile`** *<file name>* **`protocol {tftp|sftp} mgt`** Unlocks 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: o`46Port` o`64Port` **Note**: You must upgrade to `46Port` port mode before you can upgrade to `64Port` port mode. **Command mode:** FOD Key mode Use the following command to perform the same action, regardless the command mode: **`copy tftp software-key address`** *<hostname or IP address>* **`keyfile`** *<file name>* **`mgt`**
`ptkey address` *<hostname or IP address>* **`key`** *<feature name>* **`protocol {tftp|sftp} file`** *<file name>* **`mgt`** Loads the specified key file to a server. **Command mode:** FOD Key mode Use the following command to perform the same action, regardless the command mode: **`copy software-key address`** *<hostname or IP address>* **`key`** *<file name>* **`protocol {tftp|sftp} file`** *<file name>* **`mgt`**

Table 378. *Feature on Demand Key Options*

Command Syntax and Usage
invkeys address *<hostname or IP address>* **invfile** *<file name>* **protocol {tftp|sftp} mgt** Loads key code inventory information to a server. **Command mode:** FOD Key mode Use the following command to perform the same action, regardless the command mode: **copy invkeys address** *<hostname or IP address>* **invfile** *<file name>* **protocol {tftp|sftp} mgt**
rmkey key *<feature name>* Removes the specified software feature. **Command mode:** FOD Key mode
exit Exit from Feature on Demand Key mode. **Command mode:** FOD Key mode
show software-key Shows software licensing keys. **Command mode:** All

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.

Stacking Boot Options

The Stacking Boot options are used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see "Stacking Configuration" on page 340.

Table 379 lists the Boot Stacking command options.

Table 379. *Boot Stacking Options*

Command Syntax and Usage
`boot stack mode [master|member] [`*<1-16>***`|all|backup|master]`** Configures the Stacking mode for the selected switch. This can be applied for: o a specific unit `<1-16>` o `all` units o `backup` unit o `master` unit **Command mode:** Global configuration
`boot stack higig-trunk` *<list of ports>* Configures the ports used to connect the switch to the stack. **Command mode:** Global configuration
`boot stack vlan` *<VLAN number>* Configures the VLAN used for Stacking control communication. **Command mode:** Global configuration
`default boot stack [master|backup|`*<asnum (1-16)>***`|all]`** Resets the Stacking boot parameters to their default values. **Command mode:** Global configuration
`boot stack push-image {image1|image2|boot}` *<asnum (1-16)>* Pushes the selected software file from the master to the selected switch. **Command mode:** Global configuration
`boot stack enable` Enables the switch stack. **Command mode:** Global configuration

Table 379. *Boot Stacking Options (continued)*

Command Syntax and Usage
no boot stack enable Disables the switch stack. **Command mode:** Global configuration
show boot stack [master|backup|<*asnum (1-16)*>**|all]** Displays current Stacking boot parameters. **Command mode:** All

When in stacking mode, the following stand-alone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Static multicast routes
- IGMP Querier
- Microburst detection

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

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 380. *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 381. *Netboot Options (/boot/netboot)*

Command Syntax and Usage
`[no] boot netboot enable` Enables or disables Netboot. When `enabled`, the switch boots into factory-default configuration, and attempts to download a new configuration file. **Command mode:** Global configuration
`[no] boot netboot tftp` *<IP address>* Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is disabled, 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

Flexible Port Mapping

Depending on the license keys installed on the switch, only a limited number of physical ports might be active. Flexible Port Mapping allows you to alter the default configuration set up by the license, by manually setting up which ports are active or inactive.

Active ports may not collectively exceed the bandwidth limit imposed by the current license level.

Table 382 lists the Flexible Port Mapping command options.

Table 382. *Flexible Port Mapping Options*

Command Syntax and Usage
`[no] boot port-map` *<port no.>* Enables or disables the specified ports. **Command mode:** Global configuration
`default boot port-map` Reverts the port mapping to the default licensed configuration. **Command mode:** Global configuration
`show boot port-map` Displays the total bandwidth available, current port mapping and configured port mapping. **Command mode:** All

The switch must be reset for port mapping changes to take effect.

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 383. *Netboot Options (/boot/qsfp-40Gports)*

Command Syntax and Usage
[no] boot qsfp-40Gports *<ports>* 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.

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, SFTP or TFTP server on your network
- Transferring the new image from the FTP, SFTP 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 an FTP/SFTP/TFTP server on your network
- The hostname or IP address of the FTP/SFTP/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:

```
CN 4093# copy {ftp|tftp|sftp} {image1|image2|boot-image} [extm-port|
mgt-port|data-port]
```

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

2. Enter the hostname or IP address of the FTP, SFTP 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, SFTP 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:

```
CN 4093(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, SFTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
CN 4093# copy {image1|image2|boot-image} {ftp|tftp|sftp}
[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, SFTP 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, SFTP 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 6.5.0
 that was downloaded at  0:23:39 Thu Jan  1, 2010
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 1.90.90.95.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the 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:

```
CN 4093(config)# boot configuration-block {active|backup|factory}
```

Rebooting 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:

```
CN 4093# 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) ?
```

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 upgrade.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift + B>**. The Boot Management menu appears.

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

Boot Management Menu
        I - Change booting image
        C - Change configuration block
        R - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        Q - Reboot
        E - Exit
Please choose your menu option:
```

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

- To change the booting image, press `I` and follow the screen prompts.
- To change the configuration block, press `C` and follow the screen prompts.
- To boot in recovery mode, press `R`. For more details, see "Boot Recovery Mode" on page 580.
- To restart the boot process from the beginning, press `Q`.
- To exit the Boot Management menu, press `E`. The booting process continues.

Boot Recovery Mode

The Boot Recovery Mode allows you to recover from a failed software or boot image upgrade using TFTP or XModem download.

To enter Boot Recovery Mode you must select "Boot in recovery mode" option from the Boot Management Menu.

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

Option? :
```

The Boot Recovery Mode menu allows you to perform the following actions:

- To recover from a failed software or boot image upgrade using TFTP, press T and follow the screen prompts. For more details, see "Recover from a Failed Image Upgrade using TFTP" on page 581.
- To recover from a failed software or boot image upgrade using XModem download, press X and follow the screen prompts. For more details, see "Recovering from a Failed Image Upgrade using XModem Download" on page 583.
- To enable the loading of an unofficial image, press P and follow the screen prompts. For more details, see "Physical Presence" on page 585.
- To restart the boot process from the beginning, press R.
- To exit Boot Recovery Mode menu, press E. The boot process continues.

Recover from a Failed Image Upgrade using TFTP

Use the following procedure to recover from a failed image upgrade using TFTP:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, CRT, PuTTY) and input the proper hostname (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. To start the recovery process using TFTP, select T. The following message will appear:

```
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
```

6. Enter the type of management port to be used:

```
Which mgmt port to be used? Internal/External:
```

7. Enter the IP address of the management port:

```
IP addr :
```

8. Enter the network mask of the management port:

```
Netmask :
```

9. Enter the gateway of the management port:

```
Gateway :
```

10. Enter the IP address of the TFTP server:

```
Server addr:
```

11. Enter the filename of the image:

```
Image Filename:
```

12. If the file is a software image, enter an image number:

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

After the procedure is complete, the Recovery Mode menu will be re-displayed.

Below is an example of a successful recovery procedure using TFTP:

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

Option? : t
Performing TFTP rescue. Please answer the following questions (enter 'q'
to quit):
Which mgmt port to be used? Internal/External: internal
IP addr :10.241.6.4
Netmask :255.255.255.128
Gateway :10.241.6.66
Server addr:10.72.97.135
Image Filename: CN4093-8.2.1.0_OS.img
        Netmask : 255.255.255.128
        Gateway : 10.241.6.66
Configuring management port.....................
Installing image CN4093-8.2.1.0_OS.img from TFTP server 10.72.97.135

Extracting images ... Do *NOT* power cycle the switch.
Installing Application: Image signature verified. Install image as image
1 or 2 (hit return to just boot image): 2
Installing image as image2: 100%

Image2 updated succeeded
Updating install log. File CN4093-8.2.1.0_OS.img installed from
10.72.97.135 at 15:29:30 on 12-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        R) Reboot
        E) Exit

Option? :
```

Recovering from a Failed Image Upgrade using XModem Download

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

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, 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. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. Select X for Xmodem download. You will see the following display:

```
Running xmodem rescue.....
```

6. When you see the following message, change the Serial Port speed to 115200 bps:

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

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

```
... Waiting for the <Enter> key to be hit before the download can start...
CC
```

8. Select the image to download. Xmodem initiates the file transfer. When download is complete, you are asked to change the Serial Port speed back to 9600 bps:

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

9. Press **<Enter>** to start installing the image. If the file is a software image, enter the image number:

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

The image install will begin. After the procedure is complete, the Recovery Mode menu will be re-displayed.

```
Extracting images ... Do *NOT* power cycle the switch.
Installing Root Filesystem:
Image signature verified.  100%
Installing Kernel:
Image signature verified.  100%
Installing Device Tree:
Image signature verified.  100%
Installing Boot Loader:  100%
Updating install log. File image installed from xmodem at 18:06:02 on
13-3-2015
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        P) Physical presence (low security mode)
        R) Reboot
        E) Exit

Option? :
```

Boot image recovery is complete.

Physical Presence

Use the following procedure to enable the installation of unofficial images on the switch:

1. Connect a PC to the console port of the switch.
2. Open a terminal emulator program that supports Telnet protocol (for example, HyperTerminal, CRT, PuTTY) and input the proper hostname (IP address) and port to connect to the console port of the switch.
3. Boot the switch and access the Boot Management menu by pressing **<Shift + B>** while the Memory Test is in progress and the dots are being displayed.
4. Enter Boot Recovery Mode by selecting R. The Recovery Mode menu will appear.
5. To begin the Physical Presence procedure, select P. The following warning message will appear:

```
WARNING: the following test is used to determine physical presence and if
completed will put the switch in low security mode.
```

6. You will be prompted for confirmation:

```
Do you wish to continue y/n?
```

7. A security test will be performed. The system location (blue) LED will blink a number of times between 1 and 12. Enter that number:

```
Hit a key to start the test. The blue location LED will blink a number of
times.

...........
How many times did the LED blink?
```

8. After entering the correct number, the Recovery Mode menu will re-appear. To install an unofficial image use one of the following procedures:
   - TFTP (for details, see page 581)
   - XModem Download (for details, see page 583)

   Note: You have three attempts to successfully complete the security test. After three incorrect attempts, the switch will reboot.

   Note: After the test is completed, the switch will be put in low security mode. This mode will allow you to install unofficial images on the switch. To revert to normal security mode, you must reboot the switch or press P again in the Recovery Mode menu.

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 384. *General Maintenance Commands*

Command Syntax and Usage
copy flash-dump ftp [data-port|extm-port|mgt-port] Saves the system dump information via FTP. For details, see page 603. **Command mode:** All except User EXEC
copy flash-dump sftp [data-port|extm-port|mgt-port] Saves the system dump information via SFTP. For details, see page 603. **Command mode:** All except User EXEC
copy flash-dump tftp [address|data-port|extm-port| |filename|mgt-port] Saves the system dump information via TFTP. For details, see page 603. **Command mode:** All except User EXEC
show flash-dump-uuencode Displays dump information in uuencoded format. For details, see page 602. **Command mode:** All
clear flash-dump Clears dump information from flash memory. **Command mode:** All except User EXEC
copy log sftp [data-port|extm-port|mgt-port] Saves the system log file (SYSLOG) via SFTP. **Command mode:** All except User EXEC
copy log tftp [address|data-port|filename|mgt-port] Saves the system log file (SYSLOG) via TFTP. **Command mode:** All except User EXEC

Table 384. *General Maintenance Commands*

Command Syntax and Usage
copy sal sftp [data-port|extm-port|mgt-port] Saves the security audit log file via SFTP. **Note:** Not available in Stacking mode. **Command mode:** All except User EXEC
copy sal tftp [address|data-port|filename|mgt-port] Saves the security audit log file via TFTP. **Note:** Not available in Stacking mode. **Command mode:** All except User EXEC
clear sal Clears the security audit log file. **Note:** Not available in Stacking mode. **Command mode:** All except User EXEC
copy tech-support ftp [data-port|extm-port|mgt-port] Redirects the technical support dump (tsdmp) to an external FTP server. **Command mode:** All except User EXEC
copy tech-support sftp [data-port|extm-port|mgt-port] Redirects the technical support dump (tsdump) to an external SFTP server. **Commands mode:** All except User EXEC
copy tech-support tftp [address|data-port|extm-port| |filename|mgt-port] Redirects the technical support dump (tsdmp) to an external TFTP server. **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. To filter the information, use the following options: o `l2` displays only Layer 2-related information o `l3` displays only Layer 3-related information o `link` displays only link status-related information o `port` displays only port-related information **Command mode:** All except User EXEC

Forwarding Database Maintenance

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

Table 385. *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: o `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) o `xxxxxxxxxxxx` (such as `080020123456`) **Command mode:** All
show mac-address-table configured-static Displays configured static entries in the FDB. **Command mode:** All
show mac-address-table interface port *<port number or alias>* Displays all FDB entries for a particular port. **Command mode:** All
show mac-address-table multicast Displays all Multicast MAC entries in the FDB. **Command mode:** All
show mac-address-table portchannel *<trunk group number>* Displays all FDB entries for a particular trunk group. **Command mode:** All
show mac-address-table private-vlan *<VLAN number>* Displays all FDB entries on a single private VLAN. **Command mode:** All
show mac-address-table state {forward|trunk|unknown} Displays all FDB entries of a particular state. **Command mode:** All
show mac-address-table static Displays static entries in the FDB. **Command mode:** All

Table 385. *FDB Manipulation Commands (continued)*

Command Syntax and Usage
show mac-address-table vlan *<VLAN number>* Displays all FDB entries on a single VLAN. **Command mode:** All
no mac-address-table *<MAC address> <VLAN number>* Removes the specified FDB entry from the selected VLAN. **Command mode:** Global configuration
no mac-address-table multicast {*<MAC address>***|all}** Removes static multicast FDB entries. **Command mode:** Global configuration
no mac-address-table static {*<MAC address>***|all}** Removes static FDB entries. **Command mode:** Global configuration
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: Lenovo 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 386. *Miscellaneous Debug Commands*

Command Syntax and Usage
debug debug-flags This command sets the flags that are used for debugging purposes. **Command mode:** All except User EXEC
debug dumpbt Displays the backtrace log. **Command mode:** All except User 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:** All except User EXEC
debug mp-trace Displays the Management Processor trace buffer. Header information similar to the following is shown: `MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748` The buffer information is displayed after the header. **Command mode:** All except User EXEC

Table 386. *Miscellaneous Debug Commands*

Command Syntax and Usage
[no] debug lacp packet {receive|transmit|both} port *<port alias or numbers>* Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on specific ports running LACP. The following parameters are available: o `receive` filters only LACP packets received o `transmit` filters only LACP packets sent o `both` filters LACP packets either sent or received By default, LACP debugging is `disabled`. **Command mode:** All except User 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: o `receive` filters only BPDU frames received o `transmit` filters only BPDU frames sent By default, STP BPDU debugging is `disabled`. **Command mode**: All except User EXEC
[no] debug ssh client {all|state} Enables or disables SSH client based debug messages. o `all:` Enables or disables all SSH client debug messages o `state:` Enables or disables SSH client state debug messages **Command mode:** All except User EXEC
[no] debug ssh server {all|disconnect|msg|packet|state} Enables or disables SSH server based debug messages. o `all:` Enables or disables all SSH server debug messages. o `disconnect:` Enables or disables SSH server disconnect debug messages o `msg:` Enables or disables SSH server type and protocol debug messages o `packet:` Enables or disables SSH server type, protocol and packet debug messages o `state:` Enables or disables SSH server state debug messages **Command mode:** All except User EXEC
[no] debug tacacs-client Enables or disables TACACS+ client based debug messages. **Command mode:** All except User EXEC
clear flash-config Deletes all flash configuration blocks. **Command mode:** All except User EXEC

IP Security Debugging

The following table describes the options available.

Table 387. *IP Security Debug Options*

Command Syntax and Usage
[no] debug sec all Enables or disables all IP security debug messages. **Command mode**: All except User EXEC
[no] debug sec crypto Enables or disables all IP security cryptographic debug messages. **Command mode**: All except User EXEC
[no] debug sec ike Enables or disables all IP security IKEv2 debug messages. **Command mode**: All except User EXEC
[no] debug sec info Displays the current security debug settings. **Command mode**: All except User EXEC
[no] debug sec ipsec Enables or disables all IPsec debug messages. **Command mode**: All except User EXEC

ARP Cache Maintenance

The following table displays ARP Cache maintenance commands.

Table 388. *Address Resolution Protocol Maintenance Commands*

Command Syntax and Usage
show ip arp Shows all ARP entries. **Command mode:** All except User EXEC
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 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 vlan *<VLAN number>* Shows ARP entries on a single VLAN. **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 94.

IP Route Manipulation

The following table displays IP Route maintenance commands.

Table 389. *IP Route Manipulation Commands*

Command Syntax and Usage
show ip route [all] Shows all routes. **Command mode:** All
show ip route address *<IP address>* Shows a single route by destination IP address. **Command mode:** All
show ip route gateway *<IP address>* Shows routes to a default gateway. **Command mode:** All
show ip route interface *<IP interface>* Shows routes on a single interface. **Command mode:** All
show ip route tag {address|bgp|broadcast|fixed|martian| |multicast|ospf|rip|static} Shows routes of a single tag. For a description of IP routing tags, see Table 42 on page 92. **Command mode:** All
show ip route type {broadcast|direct|indirect|local| |martian|multicast} Shows routes of a single type. For a description of IP routing types, see Table 41 on page 92. **Command mode:** All
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 91.

LLDP Cache Manipulation

Table 390 describes the LLDP cache manipulation commands.

Table 390. *LLDP Cache Manipulation commands*

Command Syntax and Usage
show lldp [information] Displays all LLDP information. **Command mode:** All
show lldp port *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
show lldp receive Displays information about the LLDP receive state machine. **Command mode:** All
show lldp remote-device [*<1-256>***|detail]** Displays information received from LLDP -capable devices. For more information, see page 68. **Command mode:** All
show lldp transmit Displays information about the LLDP transmit state machine. **Command mode:** All
clear lldp Clears the LLDP cache. **Command mode:** All except User EXEC

IGMP Group Maintenance

Table 391 describes the IGMP group maintenance commands.

Table 391. *IGMP Multicast Group Maintenance Commands*

Command Syntax and Usage
show ip igmp groups Displays information for all multicast groups. **Command mode:** All
show ip igmp groups address *<IP address>* Displays a single IGMP multicast group by its IP address. **Command mode:** All
show ip igmp groups detail *<IP address>* Displays detailed information about a single IGMP multicast group. **Command mode:** All
show ip igmp groups interface port *<port number or alias>* Displays all IGMP multicast groups on selected ports. **Command mode:** All
show ip igmp groups portchannel *<trunk number>* Displays all IGMP multicast groups on a single trunk group. **Command mode:** All
show ip igmp groups vlan *<VLAN number>* Displays all IGMP multicast groups on a single VLAN. **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 392. *IGMP Multicast Router Maintenance Commands*

Command Syntax and Usage
show ip igmp mrouter Displays information for all Mrouters. **Command mode:** All
show ip igmp mrouter dynamic Displays all dynamic multicast router ports installed. **Command mode:** All
show ip igmp mrouter information Displays IGMP snooping information for all Mrouters. **Command mode:** All
show ip igmp mrouter interface port *<port alias or number>* Displays all multicast router ports installed on a specific port. **Command mode:** All
show ip igmp mrouter portchannel *<trunk number>* Displays all multicast router ports installed on a specific portchannel group. **Command mode:** All
show ip igmp mrouter static Displays all static multicast router ports installed. **Command mode:** All
show ip igmp mrouter vlan *<VLAN number>* Displays IGMP Mrouter information for a single VLAN. **Command mode:** All
show ip igmp relay Displays IGMP relay information. **Command mode:** All
show ip igmp snoop [igmpv3] Displays IGMP snooping information. The `igmpv3` option displays IGMPv3 snooping information. **Command mode:** All
clear ip igmp mrouter Clears the IGMP Mrouter port table. **Command mode:** All except User EXEC

MLD Multicast Group Manipulation

Table 393 describes the Multicast Listener Discovery (MLD) manipulation options.

Table 393. *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 dynamic Clears all dynamic MLD 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 mrouter Clears all dynamic MLD multicast router group tables. **Command mode:** All except User EXEC

IPv6 Neighbor Discovery Cache Manipulation

Table 394 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 394. *IPv6 Neighbor Discovery cache manipulation commands*

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

IPv6 Route Maintenance

Table 395 describes the IPv6 route maintenance commands.

Table 395. *IPv6 Route Maintenance Options*

Command Syntax and Usage
show ipv6 route Shows all IPv6 routes. **Command mode:** All
show ipv6 route address *<IPv6 address>* Show a single route by destination IP address. **Command mode:** All
show ipv6 route gateway *<IPv6 gateway number>* Show routes to a single gateway. **Command mode:** All
show ipv6 route interface *<interface number>* Show routes on a single IP interface. **Command mode:** All
show ipv6 route static Show static IPv6 routes. **Command mode:** All
show ipv6 route summary Shows a summary of IPv6 route information. **Command mode:** All
show ipv6 route type {connected|static|ospf} Show routes of a single type. **Command mode:** All
clear ipv6 route Clears all IPv6 routes. **Command mode: All except** User 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 604.

To access dump information, enter:

```
CN 4093# show flash-dump-uuencode
```

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

```
No FLASH dump available.
```

TFTP, SFTP or FTP System Dump Copy

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:

```
CN 4093# copy flash-dump tftp [address|data-port|extm-port|filename|
|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 SFTP, enter:

```
CN 4093# copy flash-dump sftp [data-port|extm-port|mgt-port]<server filename>
```

You are prompted for the SFTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
CN 4093# 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:

```
CN 4093# 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, 2010. 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. Lenovo N/OS System Log Messages

The CN4093 10Gb Converged Scalable Switch (CN4093) uses the following syntax when outputting system log (syslog) messages:

<Time stamp> <IP/Hostname> <Log Label> <Thread ID>`:` *<Message>*

The following parameters are used:

- *<Timestamp>*

  The time of the message event is displayed in the following format:

  <month (3 characters)> <day> <hour (1-24)>`:`*<minute>*`:`*<second>*

  For example: `Aug 19 14:20:30`

- *<IP/Hostname>*

  The hostname is displayed when configured.

  For example: `1.1.1.1`

- *<Log Label>*

  The following types of log messages are recorded: `LOG_CRIT`, `LOG_WARNING`, `LOG_ALERT`, `LOG_ERR`, `LOG_NOTICE` and `LOG_INFO`.

- *<Thread ID>*

  This is the software thread that reports the log message.

  For example: `stg`, `ip`, `console`, `telnet`, `vrrp`, `system`, `web server`, `ssh`, `bgp`

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as `mgmt`, one of the following may be shown: `console`, `telnet`, `web server`, or `ssh`.

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
BGP	session with <*IP address*> failed (bad event:<*event*>)
BGP	session with <*IP address*> failed <*reason*> Reasons: • Connect Retry Expire • Holdtime Expire • Invalid • Keepalive Expire • Receive KEEPALIVE • Receive NOTIFICATION • Receive OPEN • Receive UPDATE • Start • Stop • Transport Conn Closed • Transport Conn Failed • Transport Conn Open • Transport Fatal Error
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
IP	Route table full
MGMT	Maximum number of login failures (<*threshold*>) has been exceeded.
OSPF	Interface IP <*IP address*>, Interface State {Down | Loopback | Waiting | P To P | DR | BackupDR | DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down | Attempt | Init | 2 Way | ExStart | Exchange | Loading | Full | Loopback | Waiting | P To P | DR | BackupDR | DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
STP	CIST new root bridge
STP	CIST topology change detected
STP	own BPDU received from port <*port*>
STP	Port <*port*>, putting port into blocking state
STP	STG <*STG*>, new root bridge
STP	STG <*STG*>, topology change detected
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>

Thread	LOG_ALERT Message (continued)
VRRP	Received <*x*> virtual routers instead of <*y*>
VRRP	received errored advertisement from <*IP address*>
VRRP	received incorrect addresses from <*IP address*>
VRRP	received incorrect advertisement interval <*interval*> from <*IP address*>
VRRP	received incorrect VRRP authentication type from <*IP address*>
VRRP	received incorrect VRRP password from <*IP address*>
VRRP	VRRP : received incorrect IP addresses list from <*IP address*>

LOG_CRIT

Thread	LOG_CRIT Message
AUDIT	NTP: cannot contact NTP server %s
AUDIT	NTP: System clock not updated. Authentication failed
AUDIT	VRRP: received incorrect VRRP authentication from %s
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private|public key}
SYSTEM	System memory is at <*n*> percent

LOG_ERR

Thread	LOG_ERR Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX APP advertise settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX APP willing settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX PFC advertise settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX PFC willing settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX PG advertise settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX PG willing settings.
DCBX	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different DCBX state settings.
MGMT	Apply is issued by another user. Try later
MGMT	Critical Error. Failed to add Interface <*interface*>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later

Thread	LOG_ERR Message (continued)
NTP	unable to listen to NTP port
PFC	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different PFC settings.
PFC	Ports <*port alias or number*> and <*port alias or number*> in trunk group <*trunk number*> have different PFC settings for priority <*priority number*>.
STP	Cannot set "{Hello Time|Max Age|Forward Delay|Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Not enough memory!

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user <*username*>.
	System log cleared via SNMP.
AUDIT	Audit log has been cleared by %s
AUDIT	Class of service for user %s is changed
AUDIT	HTTPS has been disabled
AUDIT	HTTPS has been enabled
AUDIT	IKEv2 has been changed on this switch. E.g. DH Group 12 change to DH Group 24
AUDIT	IPsec manual policy X has been applied to interface XX. Security mode:[ESP/AH] Integrity algorithm:[xx] Encryption algorithm:[xx] Protocol mode: [tunnel/tranport]
AUDIT	IPsec manual policy X has been detached from interface XX
AUDIT	LDAP has been disabled
AUDIT	LDAP has been enabled
AUDIT	Password for %s changed by %s, notifying admin to save
AUDIT	RADIUS has been disabled
AUDIT	RADIUS has been enabled
AUDIT	SSH server has been disabled
AUDIT	SSH server has been enabled
AUDIT	Successful user login(logout)
AUDIT	TACACS+ has been disabled
AUDIT	TACACS+ has been enabled
AUDIT	Test event initiated for snmpv3 account and path verify
AUDIT	User %s is created
HOTLINKS	"Error" is set to "{Active|Standby}"
HOTLINKS	"Learning" is set to "{Active|Standby}"
HOTLINKS	"None" is set to "{Active|Standby}"
HOTLINKS	"Side Max" is set to "{Active|Standby}"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface

Thread	LOG_INFO Message (continued)
MGMT	/* Config changes at <*time*> by <*username*> */ <*config diff*> /* Done */
MGMT	<*username*> ejected from BBI
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser | BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}
MGMT	Firmware downloaded to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1 | 2 download completed. Now writing to flash.
MGMT	image1 | 2 downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	image1 | 2 downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()

Thread	LOG_INFO Message (continued)
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	invalid image downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	New config set
MGMT	new configuration applied [from BBI|EM|SCP|SNMP|Stacking Master]
MGMT	new configuration saved from {BBI|ISCLI|SNMP}
MGMT	scp <*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
MGMT	scp <*username*>(<*user type*>) login {on Console|from host <*IP address*>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	SP boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	Starting Firmware download for {invalid image|image1|image2 |boot kernel|undefined|SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	undefined downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	unsaved changes reverted [from BBI|from SNMP]
MGMT	Unsupported GBIC {accepted|refused}
MGMT	user {SNMP user|<*username*>} ejected from BBI
MGMT	Watchdog has been {enabled|disabled}
MGMT	Watchdog timeout interval is now <*seconds*> seconds)

Thread	LOG_INFO Message (continued)
MGMT	Wrong config file type
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config
SSH	New config set
SSH	scp <*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp <*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	server key autogen {starts | completes}
SSH	Wrong config file type
SYSTEM	booted version <*version*> from Flash image <*image*>, {active | backup | factory} config block

LOG_NOTICE

Thread	LOG_NOTICE Message
	ARP table is full.
	Current config successfully tftp'd <*filename*> from <*hostname*>
	Current config successfully tftp'd to <*hostname*>: <*filename*>
	Port <*port*> mode is changed to full duplex for 1000 Mbps operation.
AUDIT	DHCP: Offer was found invalid by ip configuration
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary|secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
HOTLINKS	"Error" is set to "Standby|Active"
HOTLINKS	"Learning" is set to "Standby|Active"
HOTLINKS	"None" is set to "Standby|Active"
HOTLINKS	"Side Max" is set to "Standby|Active"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface
MGMT	<*username*> automatically logged out from BBI because changing of authentication type
MGMT	<*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {BBI|Console|Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console|from host <*IP address*>|from BBI}
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI|TELNET} from host <*IP address*>.

Thread	LOG_NOTICE Message (continued)
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper|operator} changed by {SNMP user|<*username*>}, notifying admin to save.
MGMT	QSFP: Port <*port*> changed to {10G|40G}, from {BBI|SNMP|CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary|secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp <*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}
MGMT	scp <*username*>(<*user type*>) login {on Console|from host <*IP address*>}
MGMT	second syslog host changed to {this host|<*IP address*>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host|<*IP address*>}
MGMT	System clock set to <*time*>.
MGMT	System date set to <*date*>.
MGMT	Terminating BBI connection from host <*IP address*>
MGMT	User <*username*> deleted by {SNMP user|<*username*>}.
MGMT	User <*username*> is {deleted|disabled} and will be ejected by {SNMP user|<*username*>}
MGMT	User {oper|operator} is disabled and will be ejected by {SNMP user|<*username*>}.
MGMT	Wrong config file type
NTP	System clock updated

Thread	LOG_NOTICE Message (continued)
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down | Loopback | Waiting | P To P | DR | BackupDR | DR Other | Attempt | Init | 2 Way | ExStart | Exchange | Loading | Full}
SERVER	link {down | up} on port <*port*>
SSH	(remote disconnect msg)
SSH	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp <*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
SSH	scp <*username*>(<*user type*>) login {on Console | from host <*IP address*>}
SSH	Wrong config file type
SYSTEM	Change fiber GIG port <*port*> mode to full duplex
SYSTEM	Change fiber GIG port <*port*> speed to 1000
SYSTEM	Changed ARP entry for IP <*IP address*> to: MAC <*MAC address*>, Port <*port*>, VLAN <*VLAN*>
SYSTEM	Enable auto negotiation for copper GIG port: <*port*>
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
SYSTEM	Port <*port*> disabled
SYSTEM	Port <*port*> disabled due to reason code <*reason code*>

Thread	LOG_NOTICE Message (continued)
SYSTEM	rebooted (<*reason*>)[, administrator logged in] Reason: • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer
SYSTEM	Received BOOTP Offer: IP: <*IP address*>, Mask: <*netmask*>, Broadcast <*IP address*>, GW: <*IP address*>
SYSTEM	Watchdog threshold changed from <*old value*> to <*new value*> seconds
SYSTEM	Watchdog timer has been enabled
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
VRRP	virtual router <*IP address*> is now {BACKUP|MASTER}
WEB	<*username*> ejected from BBI
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_WARNING

Thread	LOG_WARNING Message
AUDIT	BGP: authentication receive error from %s
AUDIT	BGP: change neighbor %d password
AUDIT	BGP: delete BGP neighbor %d password
AUDIT	BGP: Password authentication fail
AUDIT	BGP: peer ttl set to %s
AUDIT	BGP: ttl-security on peer %s ignored packet
AUDIT	DHCP: disable
AUDIT	DHCP: enable
AUDIT	DHCP: Enabling DHCP will overwrite IP interface %d and IP gateway %d's configurations.
AUDIT	DHCP: on External Management Interface disabled with I2C Control Register
AUDIT	DHCP: on External Management Interface enabled with I2C Control Register
AUDIT	DHCP: Use factory default while requesting for a new DHCP offer.
AUDIT	Failed login attempt via the %s
AUDIT	IP: ARP table is full.
AUDIT	IP: Changed ARP entry for IP %s to:\tMAC %02x:%02x:%02x:%02x:%02x:%02x
AUDIT	IP: gateway %s is down
AUDIT	IP: gateway %s is up
AUDIT	IP: New Management Gateway %s configured
AUDIT	IP: New Management IP Address %s configured
AUDIT	IP: Route table full
AUDIT	LDAP security does not meet security strict mode requirements
AUDIT	OSPF: area %s authentication type is %s
AUDIT	OSPF: delete OSPF authentication key
AUDIT	OSPF: received incorrect authentication
AUDIT	OSPF: Route table full
AUDIT	OSPF: set OSPF authentication key %d

Thread	LOG_WARNING Message (continued)
AUDIT	OSPF: use OSPF authentication key
AUDIT	OSPFv3: authentication enable
AUDIT	OSPFv3: authentication reset to default
AUDIT	OSPFv3: authentication spi %d auth %s
AUDIT	OSPFv3: disable OSPFv3 authentication spi %d
AUDIT	OSPFv3: disable OSPFv3 encryption spi %d
AUDIT	OSPFv3: encryption enable
AUDIT	OSPFv3: encryption reset to default
AUDIT	OSPFv3: encryption spi %d esp auth %s encrypt %s
AUDIT	RADIUS security does not meet security strict mode requirements
AUDIT	RIP: change authentication key
AUDIT	RIP: delete RIP authentication
AUDIT	RIP: received incorrect authentication
AUDIT	TACACS+ security does not meet security strict mode requirements
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
MGMT	The software demo license for Upgrade2 will expire in 10 days. The switch will automatically reset to the factory configuration after the license expires. Please backup your configuration or enter a valid license key so the configuration will not be lost.
NTP	cannot contact [primary | secondary] NTP server <*IP address*>
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked

Thread	LOG_WARNING Message (continued)
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled

Appendix B. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check the IBM ServerProven website to make sure that the hardware and software is supported by your product.
- Go to the IBM Support portal to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs

- Start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties.

Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and X-Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as total bytes written (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Recycling Information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:

http://www.lenovo.com/recycling

Particulate Contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication Regulatory Statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic Emission Notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de Conformité à la Réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union 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. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Germany Class A Statement

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: “Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.”

Nach dem EMVG: Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) 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 Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein
Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln” EMVG (früher “Gesetz über die elektromagnetische Verträglichkeit von Geräten"). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:
Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: “Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: “Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.” (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

Japan VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI–A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase).

Korea Communications Commission (KCC) Statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People’s Republic of China Class A electronic emission Statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance Statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 00MY376

Printed in USA

(IP) P/N: 00MY376