Lenovo Flex System SI4091 10Gb System Interconnect Module

ISCLI—Industry Standard CLI Command Reference

For Lenovo Network Operating System 8.3

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 (September 2015)

Contents

Preface

The *Lenovo Flex System SI4091 10Gb System Interconnect Module ISCLI Command Reference* describes how to configure and use the Lenovo N/OS 8.3 software with your Lenovo Flex System SI4091 10Gb System Interconnect Module (referred to as SI4091 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 SI4091. For details about the configuration and operation of the SI4091, see the *Lenovo N/OS 8.3 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 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.

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 [***<125-128>***]** you enter **show interface ip** or **show interface ip** *<125-128>*
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 {***<1-48>***|hash|information}** you must enter: **show portchannel** *<1-48>* or **show portchannel hash** or **show portchannel information**

Chapter 1. ISCLI Basics

Your SI4091 10Gb System Interconnect Module (SI4091) 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 SI4091.

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 SI4091. 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 `SI 4091>`	Default mode, entered automatically on console Exit: **`exit`** or **`logout`**
Privileged EXEC `SI 4091#`	Enter Privileged EXEC mode, from User EXEC mode: **`enable`** Exit to User EXEC mode: **`disable`** Quit ISCLI: **`exit`** or **`logout`**
Global Configuration `SI 4091(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: **`configure terminal`** Exit to Privileged EXEC: **`end`** or **`exit`**
Interface IP `SI 4091(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: **`interface ip`** *<interface number>* Exit to Global Configuration mode: **`exit`** Exit to Privileged EXEC mode: **`end`**

Table 1. *ISCLI Command Modes (continued)*

Command Mode/Prompt	Command used to enter or exit
Interface Port `SI 4091(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 `SI 4091(config-PortChannel)#`	Enter PortChannel Configuration mode, from Global Configuration mode: **`interface portchannel {`***<portchannel number>***`|lacp`** *<key>***`}`** Exit to Privileged EXEC mode: **`exit`** Exit to Global Configuration mode: **`end`**
VLAN `SI 4091(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`**

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:

```
SI 4091(config)# vlan 1,3,4095                  (access VLANs 1, 3, and 4095)
SI 4091(config)# vlan 1-20                      (access VLANs 1 through 20)
SI 4091(config)# vlan 1-5,90-99,4090-4095       (access multiple ranges)
SI 4091(config)# 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:

```
SI 4091(config)# interface port 1-4    (access ports 1 though 4)
```

Command Abbreviation

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

```
SI 4091(config)# show mac-address-table interface port 12
```

or:

```
SI 4091(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 SI4091. 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 SI4091. 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 SI4091. 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 SI4091. 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 SI4091, 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 84. **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 85. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each external port. For details, see page 87. **Command mode:** All
`show information-dump` Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

System Information

The information provided by each command option is briefly described in Table 5 on page 26, 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 38. **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 40. **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 171. **Command mode:** All
`show line vty length` Displays the current `line vty length` setting. For details, see page 171. **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 30. **Command mode:** All
`show snmp-server v3 view` Displays information about view, subtrees, mask and type of view. To view a sample, see page 31. **Command mode:** All
`show snmp-server v3 access` Displays View-based Access Control information. To view a sample, see page 32. **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 33. **Command mode:** All
`show snmp-server v3 community` Displays information about the community table information. To view a sample, see page 33. **Command mode:** All
`show snmp-server v3 target-address` Displays the Target Address table information. To view a sample, see page 34. **Command mode:** All
`show snmp-server v3 target-parameters` Displays the Target parameters table information. To view a sample, see page 35. **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 36. **Command mode:** All
show snmp-server v3 Displays all the SNMPv3 information. To view a sample, see page 37. **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
----------   -------    ------          ------   ------   --------
mmgrp        usm        authPriv        iso      iso      iso
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          mmv3_mgr                       mmgrp
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.

Table 13. *SNMPv3 Community Table Information Parameters (continued)*

Field	Description
User Name	Displays the User Security Model (USM) user name.
Tag	Displays the community tag. This tag specifies a set of transport endpoints from which a command responder application accepts management requests and to which a command responder application sends an SNMP trap.

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

`show snmp-server v3 target-address`

Command mode: All

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

```
Name       Transport Addr               Port Taglist    Params
---------- ---------------------------- ---- ---------- ---------------
mmtaddr    fe80:0:0:0:211:25ff:fec3:9be  162  mmtag      mmtparam
```

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
--------------- --------   --------------    ---------  ---------
mmtparam        snmpv3     mmv3_mgr          usm        authPriv
```

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
------------------- --------------------
mmnotif             mmtag
```

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

```
Engine ID = 80:00:4F:4D:B1:1B:33:D6:CD:73:EE:7E:E1:45:67:A8:97:DC:97:93:00

usmUser Table:
User Name                       Protocol
------------------------------- -------------------------------
adminmd5                        HMAC_MD5, DES PRIVACY
adminsha                        HMAC_SHA, DES PRIVACY
mmv3_mgr                        HMAC_SHA, AES PRIVACY
v1v2only                        NO AUTH,  NO PRIVACY
adminshaaes                     HMAC_SHA, AES PRIVACY

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

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

vacmSecurityToGroup Table:
All active SNMPv3 groups are listed below:
Sec Model  User Name                      Group Name
---------- ------------------ ----------  ------------------------------
snmpv1     v1v2only                        v1v2grp
usm        adminmd5                        admingrp
usm        adminsha                        admingrp
usm        mmv3_mgr                        mmgrp
usm        adminshaaes                     admingrp

snmpCommunity Table:
Index            Name       User Name            Tag
---------------- ---------- -------------------- ------------

snmpNotify Table:
Name                Tag
------------------- --------------------
mmnotif             mmtag

snmpTargetAddr Table:
Name            Transport Addr               Port Taglist    Params
---------- ------------------------------- ---- --------- -------------
mmtaddr    fe80:0:0:0:211:25ff:fec3:9be     162  mmtag      mmtparam

snmpTargetParams Table:
Name                MP Model User Name            Sec Model Sec Level
------------------- -------- -------------------- --------- ------------
mmtparam            snmpv3   mmv3_mgr             usm       authPriv
```

General System Information

The following command displays system information:

`show sys-info`

Command mode: All

```
System Information at 15:16:48 Tue Mar 17, 2015
Time zone: Africa/Botswana
Daylight Savings Time Status: Disabled

Lenovo Flex System SI4091 10Gb System Interconnect Module

Switch has been up for 0 days, 21 hours, 37 minutes and 13 seconds.
Last boot: 17:43:13 Mon Mar 16, 2015 (reset from console)

MAC address: a8:97:dc:97:93:00
Internal Management Port MAC Address: a8:97:dc:97:93:ef
Internal Management Port IP Address (if 128): 10.241.42.151
External Management Port MAC Address: a8:97:dc:97:93:fe
External Management Port IP Address (if 127):

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



Hardware Part Number        : 00CG542
Hardware Revision           : 01
Serial Number               : Y031CM42J005
Manufacturing Date (WWYY)   : 0814
PCBA Part Number            : 00CG539
PCBA Revision               : 0
PCBA Number                 : 00
Board Revision              : 01
PLD Firmware Version        : 0.5

Temperature Warning         : 30 C (Warning  at 60 C / Recover at 55 C)
Temperature Shutdown        : 30 C (Shutdown at 68 C / Recover at 63 C)
Temperature Inlet           : 24 C
Temperature Exhaust         : 28 C
Temperature Asic Max        : 37 C

Power Consumption           : 24.900 W (12.332 V   2.024 A)


Switch is in I/O Module Bay 3
```

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

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.

Layer 2 Information

The following commands display Layer 2 information.

Table 19. *Layer 2 Information Commands*

Command Syntax and Usage
`show portchannel information` Displays the state of each port in the various Link Aggregation Groups (LAGs). For details, see page 57. **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 58. **Command mode:** All
`show failover trigger [`*<trigger number>***`|information]`** Displays Layer 2 Failover information. For details, see page 49. **Command mode:** All
`show hotlinks information` Displays Hot Links information. For details, see page 51. **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 16K MAC address entries on the MP per switch.

Table 20. *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 45.
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 *<LAG number>* Displays all FDB entries for a particular Link Aggregation Group (LAG). **Command mode:** All
show mac-address-table private-vlan *<VLAN number>* Displays all FDB entries on a single private VLAN. **Command mode:** All

Table 20. *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 aggregation (TRK) state, the port field represents the Link Aggregation Group (LAG) number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports 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 21. *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 323.

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the SI4091.

Table 22. *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 47. **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
--------------------------------------------------------------------------------
INT1    off        1         1     no        32768    --     --    --        1
INT2    off        2         2     no        32768    --     --    --        1
INT3    off        3         3     no        32768    --     --    --        1
INT4    off        4         4     no        32768    --     --    --        1
INT5    off        5         5     no        32768    --     --    --        1
INT6    off        6         6     no        32768    --     --    --        1
INT7    off        7         7     no        32768    --     --    --        1
INT8    off        8         8     no        32768    --     --    --        1
INT9    off        9         9     no        32768    --     --    --        1
INT10   off       10        10     no        32768    --     --    --        1
INT11   off       11        11     no        32768    --     --    --        1
INT12   off       12        12     no        32768    --     --    --        1
INT13   off       13        13     no        32768    --     --    --        1
INT14   off       14        14     no        32768    --     --    --        1
EXT1    active  1000      1000     no        32768    --    25*   down       1
EXT2    active  1000      1000     no        32768    --    25*   down       1
EXT3    active  1000      1000     no        32768    --    25*   down       1
EXT4    active  1000      1000     no        32768    --    25*   down       1
EXT5    active  1000      1000     no        32768    --    25*   down       1
EXT6    active  1000      1000     no        32768    --    25*   down       1
EXT7    active  1000      1000     no        32768    --    25*   down       1
EXT8    active  1000      1000     no        32768    --    25*   down       1
EXT9    active  1000      1000     no        32768    --    25*   down       1
EXT10   active  1000      1000     no        32768    --    25*   down       1
(*) LACP PortChannel is statically bound to the admin key
```

LACP dump includes the following information for each external port in the SI4091:

- `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 (LAG).
- `prio` Shows the value of the port priority.
- `aggr` Displays the aggregator associated with each port.
- `trunk` This value represents the LACP LAG 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 LAG.

Layer 2 Failover Information Commands

The following command displays Layer 2 Failover information:

Table 23. *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 49. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

`show failover trigger`

Command mode: All

```
Current global Failover setting: OFF
Current global VLAN Monitor settings: OFF

Current Trigger 1 setting: enabled
limit 0
Auto Monitor settings:
Manual Monitor settings:
        LACP port adminkey 1000
Manual Control settings:
         ports INT1-INT14

Current Trigger 2 setting: disabled
limit 0
Auto Monitor settings:
Manual Monitor settings:
Manual Control settings:

Current Trigger 3 setting: disabled
limit 0
Auto Monitor settings:
Manual Monitor settings:
Manual Control settings:
...
```

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

- Port link is up.
- If the port is a member of an LACP Link Aggregation Group (LAG), the port is aggregated.

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

A control port is considered to be operational if the monitor trigger state is `Up`. Even if a port's link status is `Down` 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 (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): 40

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

Active state: None

Active VLANs on Master interface: None
Active VLANs on Backup interface: 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 24. *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 25. *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 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 54. **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: 3

LocalPort|Index|Remote Chassis ID|Remote Port      |Remote System Name|DMAC
---------|-----|-----------------|-----------------|------------------|----
INT1     | 2   |00 90 fa 7d 61 cb|00-90-fa-7d-61-cb|G8052-11          |NB
INT2     | 1   |00 90 fa 7d 68 cb|00-90-fa-7d-68-cb|G8052-12          |NB
INT12    | 3   |00 90 fa 64 30 33|00-90-fa-64-30-33|G8052-13          |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: INT2
        Remote Device Index     : 1
        Remote Device TTL       : 118
        Remote Device RxChanges : false
        Chassis Type            : Mac Address
        Chassis Id              : 00-90-fa-7d-68-cb
        Port Type               : Mac Address
        Port Id                 : 00-90-fa-7d-68-cb
        Port Description        :

        System Name        :
        System Description : Emulex OneConnect 10Gb Multi function Adapter
        System Capabilities Supported : station only
        System Capabilities Enabled   : station only

Local Port Alias: INT1
        Remote Device Index     : 2
        Remote Device TTL       : 117
        Remote Device RxChanges : false
        Chassis Type            : Mac Address
        Chassis Id              : 00-90-fa-7d-61-cb
        Port Type               : Mac Address
        Port Id                 : 00-90-fa-7d-61-cb
        Port Description        :

        System Name        :
        System Description : Emulex OneConnect 10Gb Multi function Adapter
        System Capabilities Supported : station only
        System Capabilities Enabled   : station only
```

Unidirectional Link Detection Information

The following commands show unidirectional link detection information.

Table 26. *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 27. *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.

LAG Information

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

`show portchannel information`

Command mode: All

```
PortChannel 20: Enabled
Protocol - Static
Port State:
  INT10: DOWN
  INT11: DOWN
  INT12: forwarding
```

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

VLAN Information

The following commands display VLAN information.

Table 28. *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 Private VLAN status **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  INT1-EXT10
4091  Black-hole VLAN        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 Name
- Status
- Management status of the VLAN
- Port membership of the VLAN
- Private VLAN configuration

Layer 3 Information

The following commands display Layer 3 information.

Table 29. *Layer 3 Information Commands*

Command Syntax and Usage
show interface ip [<*interface number*>**]** Displays IPv4 interface information. For details, see page 72. **Command mode:** All
show ip dns Displays the current Domain Name System settings. **Command mode:** All
show ip gateway <3-4> Displays the current gateway settings. **Command mode:** All
show ip igmp Displays IGMP Information. For more IGMP information options, see page 68. **Command mode**: All
show ip information Displays all IP information. **Command mode:** All
show ip interface brief Displays IP Information. For details, see page 75. 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 route Displays all routes configured on the switch. For details, see page 63. **Command mode:** All
show ip slp Displays information about the Service Location Protocol (SLP) configuration. For command options, see page 89. **Command mode:** All

Table 29. *Layer 3 Information Commands (continued)*

Command Syntax and Usage
show ipv6 gateway6 <3-4> Displays the current IPv6 default gateway configuration. **Command mode**: All
show ipv6 interface [<*interface number*>**]** Displays IPv6 interface information. For details, see page 73. **Command mode:** All
show ipv6 neighbors Displays IPv6 Neighbor Discovery cache information. For more information options, see page 67. **Command mode**: All
show ipv6 pmtu [<*destination IPv6 address*>**]** Displays IPv6 Path MTU information. For details, see page 74. **Command mode:** All
show ipv6 route Displays IPv6 routing information. For more information options, see page 65. **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 30. *Route Information Commands*

Command Syntax and Usage
show ip route [all] Displays all routes configured in the switch. For more information, see page 63. **Command mode:** All
show ip route address *<IP address>* Displays a single route by destination IP address. **Command mode:** All
show ip route gateway *<IP address>* Displays routes to a single gateway. **Command mode:** All
show ip route interface *<interface number>* Displays routes on a single interface. **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 32 on page 63. **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 31 on page 63. **Command mode:** All

Show All IP Route Information

The following command displays IP route information:

`show ip route`

Command mode: All

```
Mgmt routes:
Status code: * - best
Destination       Mask            Gateway        Type      Tag       Metric If
----------------- --------------- -------------- --------- --------- ------ ---
* 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 31. *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 32. *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 SI4091 10Gb System Interconnect Module.
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).

Table 32. *IP Routing Tag Parameters (continued)*

Parameter	Description
bgp	The address was learned via Border Gateway Protocol (BGP).
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

IPv6 Routing Information

Table 33 describes the IPv6 Routing information options.

Table 33. *IPv6 Routing Information Commands*

Command Syntax and Usage
show ipv6 route Displays all IPv6 routing information. For more information, see page 66. **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,        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 34. *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 67. **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
```

IGMP Information

The following commands display IGMP information:

Table 35. *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 70. **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 Link Aggregation Group (LAG). **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 71. **Command mode:** All
show ip igmp mrouter [information] Displays IGMP Multicast Router information. For details, see page 71. **Command mode:** All

Table 35. *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 snoop Displays IGMP Snooping information. **Command mode:** All

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

Interface Information

The following command displays interface information:

`show interface ip`

Command mode: All

```
Interface information:
125:    IP6 0:0:0:0:0:0:0:0/0                          , vlan 4095, DISABLED

126:    IP6 0:0:0:0:0:0:0:0/0                          , vlan 4095, up
         fe80::aa97:dcff:fe7f:15ef
127:    IP4 10.241.10.50    255.255.255.128 10.241.10.127 , vlan 4095, up
128:    IP4 192.168.70.120  255.255.255.0   192.168.70.255, vlan 4095, up

Loopback interface information:
```

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

```
Interface information:
126:  IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::aa97:dcff:fe97:93ef
128:  IP4 10.241.42.151   255.255.255.128 10.241.42.255  , vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
4: 10.241.42.254,   up  active

Default IP6 gateway information:

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


Current IP forwarding settings: OFF, dirbr disabled, icmprd disabled

Current network filter settings:
  none

Current route map settings:
  none
```

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.

Quality of Service Information

The following commands display Quality of Service information.

Table 36. *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 77. **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 37. *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 38. *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.

Access Control List Information Commands

The following commands display Access Control List information.

Table 39. *ACL Information Options*

Command Syntax and Usage
show access-control group [*<1-384>***]** Displays ACL group information. **Command mode:** All
show access-control list [*<1-384>***]** Displays ACL list information. For details, see page 79. **Command mode:** All
show access-control list6 [*<1-128>***]** Displays IPv6 ACL list information. **Command mode:** All

Access Control List Information

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

`show access-control list` *<1-384>*

Command mode: All

```
Current ACL information:
------------------------
  Filter 2 profile:
   Ethernet
     - VID        : 2/Oxfff
   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 40. *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 41. *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 82. **Command mode:** All
show rmon event [<*event group number*>**]** Displays RMON Event information. For details, see page 83. **Command mode:** All
show rmon history [<*history group number*>**]** Displays RMON History information. For details, see page 81. **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 42. *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 43. *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 43. *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   OD: OH: 1M:2OS  Event_1
   2  none   OD: OH: OM: OS  Event_2
   3  log    OD: OH: OM: OS  Event_3
   4  trap   OD: OH: OM: OS  Event_4
   5  both   OD: OH: OM: OS  Log and trap event for Link Down
  10  both   OD: OH: OM: OS  Log and trap event for Link Up
  11  both   OD: OH: OM: OS  Send log and trap for icmpInMsg
  15  both   OD: OH: OM: OS  Send log and trap for icmpInEchos

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

The following table describes the RMON Event Information parameters.

Table 44. *RMON Event Parameter Descriptions*

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

Link Status Information

The following command displays link information:

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

Command mode: All

```
--------------------------------------------------------------------------
Alias   Port   Speed    Duplex     Flow Ctrl      Link     Description
------- ----   -----   --------  --TX-----RX--   ------   -------------
INT1      1     10000     full     yes    yes       up        INT1
INT2      2     10000     full     yes    yes       up        INT2
INT3      3     1G/10G    full     yes    yes      down       INT3
INT4      4     10000     full     yes    yes       up        INT4
INT5      5     1G/10G    full     yes    yes      down       INT5
INT6      6     10000     full     yes    yes       up        INT6
INT7      7     1G/10G    full     yes    yes      down       INT7
INT8      8     1G/10G    full     yes    yes      down       INT8
INT9      9     1G/10G    full     yes    yes      down       INT9
INT10     10    1G/10G    full     yes    yes      down       INT10
INT11     11    1G/10G    full     yes    yes      down       INT11
INT12     12    10000     full     yes    yes       up        INT12
INT13     13    1G/10G    full     yes    yes      down       INT13
INT14     14    1G/10G    full     yes    yes      down       INT14
EXT1      15    10000     full      no     no      down       EXT1
EXT2      16    10000     full      no     no      down       EXT2
EXT3      17    10000     full      no     no      down       EXT3
EXT4      18    10000     full      no     no      down       EXT4
EXT5      19    10000     full      no     no      down       EXT5
EXT6      20    10000     full      no     no      down       EXT6
EXT7      21    10000     full      no     no      down       EXT7
EXT8      22    10000     full      no     no      down       EXT8
EXT9      23    10000     full      no     no      down       EXT9
EXT10     24    10000     full      no     no      down       EXT10
EXTM      25      any     auto     yes    yes      down       EXTM
MGT1      26     1000     full     yes    yes       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 SI4091, 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 RMON Lrn Fld PVID     DESCRIPTION       VLAN(s)
              Trk              NVLAN
-------- ---- --- ---- --- --- ------ -------------- --------------------
INT1     1     n   d    e   e     1#  INT1           1
INT2     2     n   d    e   e     1#  INT2           1
INT3     3     n   d    e   e     1#  INT3           1
INT4     4     n   d    e   e     1#  INT4           1
INT5     5     n   d    e   e     1#  INT5           1
INT6     6     n   d    e   e     1#  INT6           1
INT7     7     n   d    e   e     1#  INT7           1
INT8     8     n   d    e   e     1#  INT8           1
INT9     9     n   d    e   e     1#  INT9           1
INT10    10    n   d    e   e     1#  INT10          1
INT11    11    n   d    e   e     1#  INT11          1
INT12    12    n   d    e   e     1#  INT12          1
INT13    13    n   d    e   e     1#  INT13          1
INT14    14    n   d    e   e     1#  INT14          1
EXT1     15    n   d    e   e     1#  EXT1           1
EXT2     16    n   d    e   e     1#  EXT2           1
EXT3     17    n   d    e   e     1#  EXT3           1
EXT4     18    n   d    e   e     1#  EXT4           1
EXT5     19    n   d    e   e     1#  EXT5           1
EXT6     20    n   d    e   e     1#  EXT6           1
EXT7     21    n   d    e   e     1#  EXT7           1
EXT8     22    n   d    e   e     1#  EXT8           1
EXT9     23    n   d    e   e     1#  EXT9           1
EXT10    24    n   d    e   e     1#  EXT10          1
EXTM     25    n   d    e   e  4095   EXTM           4095
MGT1     26    y   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     < NO Device Installed >
EXT3 SFP+  3  LINK  PasDAC 3.0m  BLADE NETWORKS  BN-SP-CBL-3M    Approved
EXT4 SFP+  4     < NO Device Installed >
EXT5 SFP+  5     < NO Device Installed >
EXT6 SFP+  6     < NO Device Installed >
EXT7 SFP+  7     < NO Device Installed >
EXT8 SFP+  8     < NO Device Installed >
EXT9 SFP+  9     < NO Device Installed >
EXT10 SFP+ 10    < 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
------------ --- ----- ----- ----- ----- ----- ----- ----------- -------
EXT10 SFP+ 10 Ena Down  NoFlt  3.24 40.0  287.2  0.0  SX SFP      Approved
    Blade Network  Part:BN-CKM-S-SX    Date:110225 S/N:BNTM1108QB
```

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 45. *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.

SLP Information

The following commands display information about Service Location Protocol settings:

Table 46. *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

DCBX Information Commands

The following commands display DCBX information.

Table 47. *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 48 describes the Converged Enhanced Ethernet (CEE) information options.

Table 48. *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 49 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 49. *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 97. **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 93. **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 95. **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 94. **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 96. **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
----- ---- ---------- ------- ------ ----- -----
INT1   1     enabled    0       0      0     0
INT2   2     enabled    0       0      4     2
INT3   3     enabled    0       0      0     0
INT4   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 50. *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 51. *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 52. *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 52. *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 53 describes the Enhanced Transmission Selection (ETS) information options.

Table 53. *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 54 describes the Priority Flow Control (PFC) information options.

Table 54. *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 55 describes the Fibre Channel over Ethernet (FCoE) information options.

Table 55. *FCoE Information Options*

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

FIP Snooping Information

Table 56 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options.

Table 56. *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

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 57. *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 168. **Command mode:** All
show layer3 counters Displays Layer 3 statistics. **Command mode:** All
show ntp counters Displays Network Time Protocol (NTP) Statistics. See page 165 for a sample output and a description of NTP Statistics. **Command mode:** All
show snmp-server counters Displays SNMP statistics. See page 161 for sample output. **Command mode:** All

Forwarding Database Statistics

The following commands display Forwarding Database statistics.

Table 58. *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 59. *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 109 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 110 for sample output. **Command mode:** All
show interface port *<port alias or number>* **interface-counters** Displays interface statistics for the specified port. See page 113 for sample output. **Command mode:** All
show interface port *<port alias or number>* **ip-counters** Displays IP statistics for the specified port. See page 116 for sample output. **Command mode:** All
show interface port *<port alias or number>* **link-counters** Displays link statistics for the specified port. See page 116 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
show interface port *<port alias or number>* **maintenance-counters** Displays maintenance statistics for the specified port. **Command mode:** All

Table 59. *Port Statistics Commands*

Command Syntax and Usage
`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 117 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

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 60. *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 61. *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 61. *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 61. *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 62. *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 62. *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 62. *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 63. *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 64. *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 65. *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 65. *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 65. *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).

Link Aggregation Group (LAG) Statistics

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

Table 66. *LAG Statistics Commands*

Command Syntax and Usage
show interface portchannel *<trunk group number>* **interface-counters** Displays interface statistics for the LAG. For a sample output see page 120. **Command mode:** All
clear interface portchannel *<trunk group number>* **counters** Clears all the statistics on the specified LAG. **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 67. *Layer 2 Statistics Commands*

Command Syntax and Usage
show fcoe counters Displays Fibre Channel over Ethernet (FCoE) statistics. See page 160 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 122 for sample output. **Command mode:** All
show interface port *<port alias or number>* **lldp counters** Displays LLDP statistics for the specified port. See page 124 for sample output. **Command mode:** All except User EXEC
show hotlinks counters Displays Hot Links statistics. See page 123 for sample output. **Command mode:** All except User EXEC
show oam counters Displays OAM statistics. See page 125 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 68. *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 69. *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 70. *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.

Layer 3 Statistics

The following commands display Layer 3 statistics.

Table 71. *Layer 3 Statistics Commands*

Command Syntax and Usage
show ip counters Displays IP statistics. See page 128 for sample output. **Command mode:** All
show ip dns counters Displays Domain Name System (DNS) statistics. See page 138 for sample output. **Command mode:** All
show ip gea **show ip gea bucket** *<IP address>* Displays Gigabit Ethernet Aggregators (GEA) IP statistics. GEA statistics are used by service and support personnel. **Command mode:** All
show ip igmp counters Displays IGMP statistics. See page 141 for sample output. **Command mode:** All
show ip igmp vlan *<VLAN number>* **counter** Displays IGMP statistics for a specific VLAN. See page 141 for sample output. **Command mode:** All
show ip route counters Displays route statistics. See page 136 for sample output. **Command mode:** All
show ip slp counter Displays Service Location Protocol (SLP) packet statistics. See page 167 for a sample output. **Command mode:** All
show ip tcp counters Displays TCP statistics. See page 138 for sample output. **Command mode:** All
show ip udp counters Displays UDP statistics. See page 140 for sample output. **Command mode:** All

Table 71. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
show ipv6 counters Displays IPv6 statistics. See page 131 for sample output. **Command mode:** All
clear ip counters Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. **Command mode:** All except User EXEC
clear ip dns counters Clears Domain Name System (DNS) 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 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 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 72. *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 72. *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 72. *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 73 describes the IPv6 statistics.

Table 73. *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 73. *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 74. *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 74. *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 75 describes the UDP statistics.

Table 75. *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 76. *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 77. *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.

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 78. *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.

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 79. *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.

Table 79. *TCP Statistics (continued)*

Statistic	Description
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.
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 80. *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 81. *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 81. *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.

Management Processor Statistics

The following commands display Management Processor statistics.

Table 82. *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 144. **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 154. **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 155. **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 155. **Command mode:** All
show processes cpu history Displays history of CPU utilization. To view a sample output, see page 157. **Command mode:** All

Packet Statistics

The following commands display Packet statistics.

Table 83. *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 144. **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
 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
 IPv6 packets:              0                   0
 LLDP PDUs:              3987                6876
 FCoE FIP 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 84. *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 84. *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 84. *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 84. *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 85. *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 149. **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 86. *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 149. **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 87. *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 88.

Table 88. *Packet Log Parsing Options*

Command Syntax and Usage
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} 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
show mp packet parse {rx|tx} https Displays only HTTPS 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

Table 88. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
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
show mp packet parse {rx|tx} other Displays logs of all packets not explicitly selectable. **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] raw Displays raw packet buffer in addition to headers. **Command mode:** All
show mp packet parse {rx|tx} snmp Displays only SNMP packets logged. **Command mode:** All

Table 88. *Packet Log Parsing Options (continued)*

Command Syntax and Usage
show mp packet parse {rx|tx} ssh Displays only SSH packets logged. **Command mode:** All
show mp packet parse {rx|tx} tacacs Displays only TACACS packets logged. **Command mode:** All
show mp packet parse {rx|tx} 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

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
147e68O8:  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 89. *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 90. *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 12:48:06 Thu Feb  5, 2015

Total CPU Utilization: For 1 second: 0.08%
                       For 5 second: 0.33%
                       For 1 minute: 0.10%
                       For 5 minute: 0.10%

Highest CPU Utilization: thread   5 (CONS) at 12:05:11 Thu Feb  5, 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       0.03%      0.21%      0.02%      0.00%    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%      0.01%       idle
 28      SNMP       0.00%      0.00%      0.00%      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%      0.01%       idle
 35      LACP       0.01%      0.01%      0.01%      0.01%       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%      0.06%      0.01%      0.01%       idle
 40      IPV6       0.00%      0.00%      0.00%      0.01%       idle
...
```

Table 91. *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 91. *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 92. *ACL Statistics Commands*

Command Syntax and Usage
show access-control counters Displays all ACL statistics. For output sample, see page 159. **Command mode:** All
show access-control list *<1-384>* **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 meter *<1-127>* **counters** Displays ACL meter statistics. For output sample, see page 159. **Command mode:** All
clear access-control list {*<1-384>***|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
```

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 93. *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 94. *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 94. *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 94. *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 94. *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 95. *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 95. *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 96. *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 97. *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 98. *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 298. **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 299. **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} [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 [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 300. **Command mode:** All except User EXEC
`copy {sftp|tftp} public-key [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 `public-key`: client public key 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 SI4091 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:

```
SI 4091# copy running-config startup-config
```

or

```
SI 4091# 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 311.

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 99. *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 99. *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 black-hole vlan` *<VLAN ID>* Configures the Black-hole VLAN. Ports that belong to this VLAN discard all traffic. The default Black-hole VLAN is `4091`. This is also the default System Reserved VLAN. **Note:** The Black-hole VLAN must be part of the system reserved VLAN range. **Note:** External ports that aren't assigned to any data VLAN are automatically associated with the Black-hole VLAN in order to avoid broadcast storms. **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]` 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
`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

Table 99. *System Configuration Commands (continued)*

Command Syntax and Usage
system internal-VLAN *<VLAN range (2-4094)>* **[black-hole vlan** *<VLAN ID>***]** Configures a range of System Reserved VLANs. The `black-hole` option also configures the Black-hole VLAN. The default reserved VLAN is `4091`. This is also the default Black-hole VLAN. **Note:** The Black-hole VLAN must be in the configured system reserved VLAN range for the command to be valid. **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
[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

Table 99. *System Configuration Commands (continued)*

Command Syntax and Usage
`terminal dont-ask` Disables CLI confirmation prompts for the current session. The switch will choose the default answer. **Note:** When using this command any settings configured through the **`prompting`** command will be temporarily disregarded for the duration of the current session. **Command mode:** All
`no terminal dont-ask` Enables CLI confirmation prompts for the current session. **Note:** When using this command any settings configured through the **`prompting`** command will be temporarily disregarded for the duration of the current session. **Command mode:** All
`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 100. *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 101. *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 102. *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>* **[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>* **[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 102. *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
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 40. The reverse option displays the output in reverse order, from the newest entry to the oldest. **Command mode:** All

SSH Server Configuration

For the SI4091 10Gb System Interconnect Module, these commands enable Secure Shell access from any SSH client.

Table 103. *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 103. *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 104. *RADIUS Server Configuration Commands*

Command Syntax and Usage
[no] radius-server backdoor Enables or disables the RADIUS backdoor for Telnet/SSH. 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 104. *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. **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
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 105. *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 or SSH/SCP. 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 SI4091, 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 105. *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 105. *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 105. *TACACS+ Server Configuration Commands (continued)*

Command Syntax and Usage
`[no] tacacs-server secure-backdoor` Enables or disables TACACS+ secure back door access through Telnet or SSH/SCP 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
`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 106. *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 or SSH/SCP. The default setting is `disabled`. **Note:** To obtain the LDAP back door password for your SI4091, 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 106. *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 107. *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 107. *NTP Server Configuration Commands*

Command Syntax and Usage
ntp primary-server *<IP address>* **[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 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>* **[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 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>* **[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 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
ntp ipv6 secondary-server *<IPv6 address>* **[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 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

Table 107. *NTP Server Configuration Commands*

Command Syntax and Usage
`[no] ntp sync-logs` Enables or disables informational logs for NTP synchronization failures. The default setting is `enabled`. **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 108. *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 109. *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 109. *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>* 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 109. *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 110. *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 198. **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 200. **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 199. **Command mode:** Global configuration

Table 110. *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 203. **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 201. **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 202. **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 196. **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 197. **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 111. *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 111. *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 112. *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 113. *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 113. *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 114. *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 196. **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 196: `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 115. *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 196: `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 116. *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 202: `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 117. *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 196) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration

Table 117. *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 118. *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 119. *System Access Configuration Commands*

Command Syntax and Usage
`[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
`access user administrator-password` Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the SI4091, 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

Table 119. *System Access Configuration Commands (continued)*

Command Syntax and Usage
access user user-password Sets the user (user) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Note:** To disable the user account, set the password to null (no password). **Command Mode**: Global configuration
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.

Note: Management ACLs filter traffic received through data interfaces only. Management interface is not monitored.

Table 120. *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

Table 120. *Management Network Configuration Commands*

Command Syntax and Usage
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 121. *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 SI4091, 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

Table 121. *User Access Control Configuration Commands*

Command Syntax and Usage
access user eject {<*user name*>**|**<*session ID*>**}** Ejects the specified user from the SI4091. **Command mode:** Global configuration
clear line <*1-12*> Ejects the user with the corresponding session ID from the SI4091. **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 122. *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 123. *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 123. *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

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 124. *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

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 221.

Table 125. *Port Configuration Commands*

Command Syntax and Usage
`interface port` *<port alias or number>* Enter Interface port mode. **Command mode:** Global configuration
`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 the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the LAG is placed in the `down` state. **Command mode:** Interface port
`[no] reflective-relay force` Enables or disables constraint to always keep reflective relay active. The default setting is `disabled`. **Command mode:** Interface port

Table 125. *Port Configuration Commands (continued)*

Command Syntax and Usage
`[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 217.) **Command mode:** Interface port
`no shutdown` Enables the port. **Command mode:** Interface port
`[no] storm-control broadcast level pps` *<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 pps` *<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 pps` *<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
`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

Table 125. *Port Configuration Commands (continued)*

Command Syntax and Usage
`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) in case of an internal port or to the default Black-hole VLAN (`VLAN 4091`) in case of an external port. **Command mode:** Interface port/Interface portchannel
`no switchport trunk allowed vlan` Assigns the port to all available data VLANs in case of an internal port or to the Black-hole VLAN in case of an external port. **Command mode:** Interface port/Interface portchannel
`switchport trunk native vlan` *<1-4094>* Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. 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

Table 125. *Port Configuration Commands (continued)*

Command Syntax and Usage
`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
`[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 126. *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 176. **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 127. *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:

```
SI 4091# 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 SI4091 10Gb System Interconnect Module is reset. See the "Operations Commands" on page 301 for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 128. *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 129. *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 130. *Port ACL/QoS Configuration Commands*

Command Syntax and Usage
`[no] access-control group` *<1-384>* Adds or removes the specified ACL group. You can add multiple ACL groups to a port. **Command mode:** Interface port
`[no] access-control list` *<1-384>* 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

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, only LLDP settings are configurable.

Table 131. *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
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

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 SI4091 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 132. *802.1p Configuration Commands*

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

DSCP Configuration

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

Table 133. *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

Table 133. *DSCP Configuration Commands*

Command Syntax and Usage
`[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 134. *CoPP Commands*

Command Syntax and Usage
`qos protocol-packet-control packet-queue-map` *<packet queue number (0-44)> <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: – **application-cri-packets** (critical packets of various applications, such as Telnet, SSH) – **arp-bcast** (ARP broadcast packets) – **arp-ucast** (ARP unicast reply packets) – **bpdu** (Spanning Tree Protocol packets) – **cisco-bpdu** (Cisco STP packets) – **dest-unknown** (packets with destination not yet learned) – **dhcp** (DHCP packets) – **fips** (FIPS packets) – **icmp** (ICMP packets) – **igmp** (IGMP packets) – **ipv4-miscellaneous** (IPv4 packets with IP options and TTL exception) – **ipv6-nd** (IPv6 Neighbor Discovery packets) – **lacp** (LACP/Link Aggregation protocol packets) – **lldp** (LLDP packets) – **system** (system protocols, such as tftp, ftp, telnet, ssh) – **udld** (UDLD 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 134. *CoPP Commands*

Command Syntax and Usage
qos protocol-packet-control rate-limit-packet-queue *<packet queue number (0-44)> <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 (0-44)>* 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

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 220.

Table 135. *General ACL Configuration Commands*

Command Syntax and Usage
[no] access-control group *<1-384>* Configures an ACL Group. To view command options, see page 235. **Command mode:** Global configuration
[no] access-control list *<1-384>* Configures an Access Control List. To view command options, see page 226. **Command mode:** Global configuration
[no] access-control list6 *<1-128>* Configures an IPv6 Access Control List. To view command options, see page 231. **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 136. *ACL Configuration Commands*

Command Syntax and Usage
access-control list *<1-384>* **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 *<1-384>* **egress-port port** *<port alias or number>* Configures the ACL to function on egress packets. **Command mode:** Global configuration
[no] access-control list *<1-384>* **statistics** Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration
default access-control list *<1-384>* Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list *<1-384>* 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 231. **Command mode:** Global configuration

Ethernet Filtering Configuration

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

Table 137. *Ethernet Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control list *<1-384>* **ethernet destination-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the destination MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list *<1-384>* **ethernet source-mac-address** *<MAC address>* **[***<MAC mask>***]** Defines the source MAC address for this ACL. **Command mode:** Global configuration
[no] access-control list *<1-384>* **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 *<1-384>* **ethernet vlan** *<VLAN ID>* **[***<VLAN mask>***]** Defines a VLAN number and mask for this ACL. **Command mode:** Global configuration
[no] access-control list *<1-384>* **ethernet priority** *<0-7>* Defines the Ethernet priority value for the ACL. **Command mode:** Global configuration
default access-control list *<1-384>* **ethernet** Resets Ethernet parameters for the ACL to their default values. **Command mode:** Global configuration
no access-control list *<1-384>* **ethernet** Removes Ethernet parameters for the ACL. **Command mode:** Global configuration
show access-control list *<1-384>* **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 138. *IP version 4 Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control list *<1-384>* **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 *<1-384>* **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 *<1-384>* **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 *<1-384>* **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 *<1-384>* **ipv4** Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-384>* **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 139. *TCP/UDP Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control list *<1-384>* **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 *<1-384>* **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 *<1-384>* **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 *<1-384>* **tcp-udp** Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-384>* **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 140. *Packet Format Filtering Configuration Commands*

Command Syntax and Usage
[no] access-control list *<1-384>* **packet-format ethernet {ethertype2|llc|snap}** Defines the Ethernet format for the ACL. **Command mode:** Global configuration
[no] access-control list *<1-384>* **packet-format ip {ipv4|ipv6}** Defines the IP format for the ACL. **Command mode:** Global configuration
[no] access-control list *<1-384>* **packet-format tagging {any|none|tagged}** Defines the tagging format for the ACL. **Command mode:** Global configuration
default access-control list *<1-384>* **packet-format** Resets Packet Format parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list *<1-384>* **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 141. *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 142. *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 143. *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 144. *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** *<64-10000000>* Configures the committed rate, in kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
[no] access-control 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

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 145. *ACL Group Configuration Commands*

Command Syntax and Usage
[no] access-control group *<1-384>* **list** *<1-384>* Adds or removes the selected ACL to/from the ACL group. **Command mode:** Global configuration
[no] access-control group *<1-384>* **list6** *<1-128>* Adds or removes the selected IPv6 ACL to/from the ACL group. **Command mode:** Global configuration
show access-control group *<1-384>* 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 146. *ACL Metering Configuration Commands*

Command Syntax and Usage
access-control list *<1-384>* **meter action {drop|pass}** Configures the ACL meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
access-control list *<1-384>* **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 *<1-384>* **meter enable** Enables or disables ACL Metering. **Command mode:** Global configuration
access-control list *<1-384>* **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 *<1-384>* **meter** Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
no access-control list *<1-384>* **meter** Deletes the selected ACL meter. **Command mode:** Global configuration
show access-control list *<1-384>* **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 147. *ACL Re-Marking Configuration Commands*

Command Syntax and Usage
access-control list *<1-384>* **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 *<1-384>* **re-mark dot1p** Disables use of 802.1p value for re-marked packets. **Command mode:** Global configuration
[no] access-control list *<1-384>* **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 *<1-384>* **re-mark** Sets the ACL Re-mark configuration to its default values. **Command mode:** Global configuration
show access-control list *<1-384>* **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 148. *ACL Re-Mark In-Profile Commands*

Command Syntax and Usage
access-control list *<1-384>* **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 *<1-384>* **re-mark in-profile dscp** Disables use of DSCP value for in-profile traffic. **Command mode:** Global configuration
no access-control list *<1-384>* **re-mark in-profile** Removes all re-mark in-profile settings. **Command mode:** Global configuration
show access-control list *<1-384>* **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 149. *ACL Re-Mark Out-of-Profile Commands*

Command Syntax and Usage
access-control list *<1-384>* **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 *<1-384>* **re-mark out-profile** Removes all re-mark out-profile settings. **Command mode:** Global configuration
show access-control list *<1-384>* **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 150. *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 151. *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 152. *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 SI4091, see "Appendix A: Troubleshooting" in the *Lenovo N/OS 8.3 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 153. *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 154. *Port-Based Port Mirroring Configuration Commands*

Command Syntax and Usage
port-mirroring monitor-port *<port alias or number>* **mirroring-port** *<port alias or number>* **{in|out|both}** Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port. If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port. **Command mode:** Global configuration
no port-mirroring monitor-port *<port alias or number>* **mirroring-port** *<port alias or number>* Removes the mirrored port. **Command mode:** Global configuration
show port-mirroring Displays the current settings of the monitoring port. **Command mode:** All

Layer 2 Configuration

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

Table 155. *Layer 2 Configuration Commands*

Command Syntax and Usage
vlan *<VLAN number>* Enter VLAN configuration mode. To view command options, see page 267. **Command mode:** Global configuration
show layer2 Displays current Layer 2 parameters. **Command mode:** All

Forwarding Database Configuration

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

Table 156. *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 157. *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 158. *FDB Configuration Commands*

Command Syntax and Usage
mac-address-table static *<MAC address>* **vlan** *<VLAN number>* **{port** *<port alias or number>***|portchannel** *<LAG 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

LLDP Configuration

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

Table 159. *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 159. *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 160. *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 161. *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 161. *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

Link Aggregation Group (LAG) Configuration

Link Aggregation Groups (LAGs) can provide super-bandwidth connections between SI4091 or other aggregation capable devices. A *LAG* is a group of ports that act together, combining their bandwidth to create a single, larger port. Two types of aggregation are available: static LAGs (portchannels) and dynamic LACP LAGs (portchannels).

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

- static LAGs: 1-24
- LACP LAGs: 25-48

Up to 24 static LAGs can be configured on the SI4091, with the following restrictions:

- Any physical switch port can belong to no more than one LAG.
- Up to 10 ports can belong to the same LAG.
- Configure all ports in a LAG with the same properties (speed, duplex, flow control, VLAN and so on).
- Aggregation from non-Lenovo devices must comply with Cisco® EtherChannel® technology and exclude the PAgP networking protocol.
- LACP LAGs should be configured to be bound to a static portchannel ID.

By default, all external ports are configured as LACP enabled with LACP key 1000 and bound to portchannel ID 25.

Table 162. *LAG Configuration Commands*

Command Syntax and Usage
`portchannel` *<1-24>* **`port`** *<port alias or number>* **`[enable]`** Adds a physical port or ports to the current LAG. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-). The `enable` option also enables the LAG. **Command mode:** Global configuration
`no portchannel` *<1-24>* **`port`** *<port alias or number>* Removes a physical port or ports from the current LAG. **Command mode:** Global configuration
`[no] portchannel` *<1-24>* **`enable`** Enables or disables the current LAG. **Command mode:** Global configuration

Table 162. *LAG Configuration Commands (continued)*

Command Syntax and Usage
no portchannel *<1-24>* Removes the current LAG configuration. **Command mode:** Global configuration
show portchannel *<1-24>* Displays current LAG parameters. **Command mode:** All

Link Aggregation Group (LAG) Hash Configuration

Use the following commands to configure Link Aggregation Group (LAG) hash settings for the SI4091. LAG hash parameters are set globally for the SI4091. The LAG hash settings affect both static LAGs and LACP LAGs.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in Table 163 combined with the hash parameters listed in Table 165.

Table 163. *LAG Hash Settings*

Command Syntax and Usage
`[no] portchannel thash ingress` Enables or disables use of the ingress port to compute the LAG 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 LAG hash configuration. **Command mode**: All

FCoE LAG Hash Configuration

Use the following commands to configure FCoE LAG Hash parameters for the SI4091.

Table 164. *FCoE LAG Hash Configuration Commands*

Command Syntax and Usage
[no] portchannel thash fcoe cntag-id Enables or disables FCoE LAG hashing on the cntag id. **Command mode:** Global configuration
[no] portchannel thash fcoe destination-id Enables or disables FCoE LAG hashing on the destination id. **Command mode:** Global configuration
[no] portchannel thash fcoe fabric-id Enables or disables FCoE LAG hashing on the fabric id. **Command mode:** Global configuration
[no] portchannel thash fcoe originator-id Enables or disables FCoE LAG hashing on the originator id. **Command mode:** Global configuration
[no] portchannel thash fcoe responder-id Enables or disables FCoE LAG hashing on the responder id. **Command mode:** Global configuration
[no] portchannel thash fcoe source-id Enables or disables FCoE LAG hashing on the source id. **Command mode:** Global configuration
show portchannel hash Display current LAG hash configuration. **Command mode**: All

Layer 2 LAG Hash

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

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

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

Table 165. *Layer 2 LAG Hash Options*

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

Layer 3 LAG Hash

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

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

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

Table 166. *Layer 3 LAG Hash Options*

Command Syntax and Usage
`[no] portchannel thash l3thash l3-destination-ip-address` Enables or disables Layer 3 LAG hashing on the destination IP address. **Command mode:** Global configuration
`[no] portchannel thash l3thash l3-source-ip-address` Enables or disables Layer 3 LAG hashing on the source IP address. **Command mode:** Global configuration
`[no] portchannel thash l3thash l3-source-destination-ip` Enables or disables Layer 3 LAG 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 LAG hash settings. **Command mode:** All

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the SI4091.

Table 167. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
`lacp system-priority` *<1-65535>* Defines the priority value for the SI4091. 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 SI4091's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static LAGs 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 LAG, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key*. **Command mode:** Global configuration
`portchannel` *<LAG ID (25-48)>* **`lacp key`** *<1-65535>* Enables a static LACP LAG. In this mode, ports sharing the same LACP admin key can form a single LAG, with the specified `LAG ID`. The active LAG is picked based on the ports which occupy first the LAG ID. Member ports that cannot join this LAG are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic. **Command mode:** Global configuration

Table 167. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
`no portchannel` *<LAG ID (25-48)>* Deletes the specified static LACP LAG. **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 168. *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 LAG. **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 LAG. o `active` turns LACP on and set this port to active. Active ports initiate LACPDUs. o `passive` turns LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. The default value is `off`. **Command mode:** Interface port
`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/Interface portchannel

Table 168. *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. **Note:** Only one external switch port in any LACP LAG can be in the individual state whereas all internal switch ports can be in the LACP individual state. **Command mode:** Interface port/Interface portchannel
port-channel min-links *<1-16>* Set the minimum number of links for the LACP LAG to which this port belongs. If the specified minimum number of ports are not available, the LAG is placed in the `down` state. **Command mode:** Interface port
default lacp [key|mode|priority|suspend-individual] Restores the selected parameters to their default values. **Command mode:** Interface port/Interface portchannel
show interface port *<port alias or number>* **lacp** Displays the current LACP configuration for this port. **Command mode:** All

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see "High Availability" in the *Lenovo N/OS Application Guide*.

Table 169. *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 170. *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 171. *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 LAGs formed with this *admin key* will be included in the Auto Monitor. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **amon portchannel** *<LAG number>* Adds or removes a LAG 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 172. *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 LAGs formed with this *admin key* will be included in the Manual Monitor Port configuration. **Command mode:** Global configuration
`[no] failover trigger` *<1-8>* **`mmon monitor member`** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Port configuration. **Command mode:** Global configuration
`[no] failover trigger` *<1-8>* **`mmon monitor portchannel`** *<LAG number>* Adds or removes the selected LAG to the Manual Monitor Port configuration. **Command mode:** Global configuration
`show failover trigger` *<1-8>* Displays the current Failover settings. **Command mode:** All

Failover Manual Monitor Control Configuration

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

Table 173. *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 LAGs formed with this *admin key* will be included in the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control member** *<port alias or number>* Adds or removes the selected port to the Manual Monitor Control configuration. **Command mode:** Global configuration
[no] failover trigger *<1-8>* **mmon control portchannel** *<LAG number>* Adds or removes the selected LAG 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 8.3 Application Guide*.

Table 174. *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. 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` *<10-200>* 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 175. *Hot Links Trigger Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* **enable** Enables or disables the Hot Links trigger. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **forward-delay** *<0-3600>* Configures the Forward Delay interval, in seconds. The default value is `1`. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **name** *<1-32 characters>* Defines a name for the Hot Links trigger. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **preemption** Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is `enabled`. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **vlan rebalance** Equally distributes the VLANs between the Master and the Backup interfaces. **Note:** This command has effect only when the hotlinks trigger is in auto-VLAN mode. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* Deletes the Hot Links trigger. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Master Configuration

Use the following commands to configure the Hot Links Master interface.

Table 176. *Hot Links Master Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* **master adminkey** *<0-65535>* Adds or removes an LACP *admin key* to the Master interface. LACP LAGs formed with this *admin key* will be included in the Master interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **master port** *<port alias or number>* Adds or removes the selected port to the Hot Links Master interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **master portchannel** *<LAG number>* Adds or removes the selected LAG to the Master interface. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

Hot Links Backup Configuration

Use the following commands to configure the Hot Links Backup interface.

Table 177. *Hot Links Backup Configuration Commands*

Command Syntax and Usage
[no] hotlinks trigger *<1-25>* **backup adminkey** *<0-65535>* Adds or removes an LACP *admin key* to the Backup interface. LACP LAGs formed with this *admin key* will be included in the Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **backup port** *<port alias or number>* Adds or removes the selected port to the Hot Links Backup interface. **Command mode:** Global configuration
[no] hotlinks trigger *<1-25>* **backup portchannel** *<LAG number>* Adds or removes the selected LAG to the Backup interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **backup prefer auto** Configures the specified hotlinks trigger in auto-VLAN mode, which automatically distributes VLANs between the Master and the Backup interfaces. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **backup prefer vlan** *<VLAN ID>* Configures the specified hotlinks trigger in preferred-VLAN mode and sets the preferred-VLAN list to the Backup interface. **Command mode:** Global configuration
hotlinks trigger *<1-25>* **backup prefer vlan {add|remove}** *<VLAN ID>* Adds or removes a VLAN to/from the Backup interface preferred-VLAN list. **Command mode:** Global configuration
no hotlinks trigger *<1-25>* **backup prefer** Configures the specified hotlinks trigger in port-based mode and clears the Backup interface preferred-VLAN configuration. **Command mode:** Global configuration
show hotlinks trigger *<1-25>* Displays the current Hot Links trigger settings. **Command mode:** All

VLAN Configuration

These commands configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

Up to 4094 VLANs can be configured on the SI4091. VLANs can be assigned any number between 1 and 4094, except the reserved VLANs.

Table 178. *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 178. *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
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
show vlan information Displays the current VLAN configuration. **Command mode:** All

Note: All ports must belong to at least one VLAN. Any internal port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. Any external ports that are not assigned to any VLAN are automatically added to the Black-hole VLAN. You cannot add a port to more than one VLAN unless the port has VLAN tagging turned **on**.

Private VLAN Configuration

Use the following commands to configure Private VLAN.

Table 179. *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 180. *Layer 3 Configuration Commands*

Command Syntax and Usage
`interface ip` *<interface number>* Configures the IP Interface. The SI4091 supports up to 4 IP interfaces: 125, 126 for IPv6 and 127, 128 for IPv4. To view command options, see page 271. **Command mode:** Global configuration
`show layer3` Displays the current IP configuration. **Command mode:** All

IP Interface Configuration

The SI4091 supports up to 4 IP interfaces: 125, 126 for IPv6 and 127, 128 for IPv4. Each IP interface represents the SI4091 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 SI4091, use the management module interface to change the IP address of the switch.

Table 181. *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 181. *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 interface ip *<interface number>* Removes this IP interface. **Command mode:** Interface IP
show interface ip *<interface number>* Displays the current interface settings. **Command mode:** All

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

Table 182. *IPv6 Neighbor Discovery Configuration Options*

Command Syntax and Usage
[no] ipv6 nd advmtu Enables or disables the MTU option in Router Advertisements. The default setting is `enabled`. **Command mode:** Interface IP
[no] ipv6 nd dad-attempts *<1-10>* Configures the maximum number of duplicate address detection attempts. The default value is `1`. **Command mode:** Interface IP

Table 182. *IPv6 Neighbor Discovery Configuration Options (continued)*

Command Syntax and Usage
[no] ipv6 nd hops-limit *<0-255>* Configures the Router Advertisement hop limit. The default value is 64. **Command mode:** Interface IP
[no] ipv6 nd managed-config Enables or disables the managed address configuration flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default setting is disabled. **Command mode:** Interface IP
[no] ipv6 nd other-config Enables or disables the other stateful configuration flag, which allows the interface to use DHCP for other stateful configuration. The default setting is disabled. **Command mode:** Interface IP
[no] ipv6 nd ra-interval *<4-1800>* Configures the Router Advertisement maximum interval. The default value is 600. **Note**: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval. **Command mode:** Interface IP
[no] ipv6 nd ra-intervalmin *<3-1350>* Configures the Router Advertisement minimum interval. The default value is 198. **Note**: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval. **Command mode:** Interface IP
ipv6 nd ra-lifetime *<0-9000>* Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (advint). The default value is 1800. **Command mode:** Interface IP
[no] ipv6 nd reachable-time *<1-3600>* **[no] ipv6 nd reachable-time** *<1-3600000>* **ms** Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is 30. **Command mode:** Interface IP

Table 182. *IPv6 Neighbor Discovery Configuration Options (continued)*

Command Syntax and Usage
[no] ipv6 nd retransmit-time *<0-4294967>* **[no] ipv6 nd retransmit-time** *<0-4294967295>* **ms** Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is `1`. **Command mode:** Interface IP
[no] ipv6 nd suppress-ra Enables or disables IPv6 Router Advertisements on the interface. The default setting is `disabled` (suppress Router Advertisements). **Command mode:** Interface IP

Default Gateway Configuration

The switch can be configured with up to 2 IPv4 gateways. Gateways 3–4 are reserved for default gateways.

Default gateway indices are:

- 3: External management gateway
- 4: Internal management gateway

This option is disabled by default.

Table 183. *Default Gateway Configuration Commands*

Command Syntax and Usage
ip gateway *<3-4>* **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 *<3-4>* **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 *<3-4>* **enable** Enables or disables the gateway for use. **Command mode:** Global configuration
ip gateway *<3-4>* **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 *<3-4>* **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 *<3-4>* Deletes the gateway from the configuration. **Command mode:** Global configuration
show ip gateway *<3-4>* Displays the current gateway settings. **Command mode:** All

IGMP Configuration

Table 184 describes the commands used to configure basic IGMP parameters.

Table 184. *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" on page 277
- "IGMPv3 Configuration" on page 278
- "IGMP Static Multicast Router Configuration" on page 281
- "IGMP Filtering Configuration" on page 279
- "IGMP Advanced Configuration" on page 282

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 185 describes the commands used to configure IGMP Snooping.

Table 185. *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 186 describes the commands used to configure IGMP version 3.

Table 186. *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 Filtering Configuration

Table 187 describes the commands used to configure an IGMP filter.

Table 187. *IGMP Filtering Configuration Commands*

Command Syntax and Usage
ip igmp profile *<1-16>* Configures the IGMP filter. To view command options, see page 279. **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 188 describes the commands used to define an IGMP filter.

Table 188. *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 189 describes the commands used to configure a port for IGMP filtering.

Table 189. *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 Static Multicast Router Configuration

Table 190 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 190. *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 191 describes the commands used to configure advanced IGMP parameters.

Table 191. *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

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 192. *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

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateways 3 and 4 are used for management traffic.

Table 193 describes the IPv6 Default Gateway Configuration commands.

Table 193. *IPv6 Default Gateway Configuration Commands*

Command Syntax and Usage
ip gateway6 <*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 <*3-4*> **enable** Enables or disables the default gateway. **Command mode**: Global configuration
no ip gateway6 <*3-4*> Deletes the default gateway. **Command mode**: Global configuration
show ipv6 gateway6 <*3-4*> Displays the current IPv6 default gateway 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 194. *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

Converged Enhanced Ethernet Configuration

Table 195 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 195. *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 196 describes the global ETS Priority Group configuration options.

Table 196. *Global ETS Priority Group Commands*

Command Syntax and Usage
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
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 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 197 describes the global PFC Priority Group configuration options.

Table 197. *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 198 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 198. *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 199 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 199. *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 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 200 describes the FCoE configuration options.

Table 200. *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
`show fcoe information` Displays the current FCoE parameters. **Command mode**: All

FIPS Port Configuration

FIP Snooping allows the switch to monitor FCoE Initialization Protocol (FIP) frames to gather discovery, initialization, and maintenance data. This data is used to automatically configure ACLs that provide FCoE connections and data security.

Table 201 describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 201. *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 202 describes the RMON History commands.

Table 202. *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 202. *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 203 describes the RMON Event commands.

Table 203. *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 204 describes the RMON Alarm commands.

Table 204. *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 204. *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

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 SI4091 10Gb System Interconnect Module behaves as a Service Agent providing systems management services.

Table 205. *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:

```
SI 4091(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 300.

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:

```
SI 4091(config)# copy running-config ftp [extm-port|mgt-port]
```

or:

```
SI 4091(config)# copy running-config tftp [extm-port|mgt-port]
```

or:

```
SI 4091(config)# copy running-config sftp [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:

```
SI 4091(config)# copy ftp running-config [extm-port|mgt-port]
```

or:

```
SI 4091(config)# copy tftp running-config [extm-port|mgt-port]
```

or:

```
SI 4091(config)# copy sftp running-config [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 206. *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 207. *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 *<1-48>* **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

Protected Mode Options

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

Table 208. *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 208. *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

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 SNMP to work with switch image and configuration files. To use SNMP, refer to "Working with Switch Images and Configuration Files" in the *Command Reference*.

The boot options are discussed in the following sections.

Scheduled Reboot

This feature allows you to schedule a reboot to occur at a particular time in the future. This feature is particularly helpful if the user needs to perform switch upgrades during off-peak hours. You can set the reboot time, cancel a previously scheduled reboot, and check the time of the currently set reboot schedule.

Table 209. *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 210. *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

Updating the Switch Software Image

The switch software image is the executable code running on the SI4091 10Gb System Interconnect Module. 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:

```
SI 4091# copy {ftp|tftp|sftp} {image1|image2|boot-image} [extm-port|
mgt-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:

```
SI 4091(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:

```
SI 4091# copy {image1|image2|boot-image} {ftp|tftp|sftp}
[extm-port|mgt-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 SI4091 10Gb System Interconnect Module, 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 SI4091 10Gb System Interconnect Module 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 SI4091 10Gb System Interconnect Module 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:

```
SI 4091(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.

Enter the following command to reset (reload) the switch:

```
SI 4091# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.
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
        1 - Change booting image
        2 - Change configuration block
        3 - Boot in recovery mode (tftp and xmodem download of images to
recover switch)
        5 - Reboot
        6 - Exit
Please choose your menu option:
```

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

- To change the booting image, press `1` and follow the screen prompts.
- To change the configuration block, press `2` and follow the screen prompts.
- To boot in recovery mode, press `3`. For more details, see "Boot Recovery Mode" on page 314.
- To restart the boot process from the beginning, press `5`.
- To exit the Boot Management menu, press `6`. 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 315.
- 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 317.
- To enable the loading of an unofficial image, press P and follow the screen prompts. For more details, see "Physical Presence" on page 319.
- 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 3. 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: SI4091-8.2.1.0_OS.img
        Netmask : 255.255.255.128
        Gateway : 10.241.6.66
Configuring management port.....................
Installing image SI4091-8.2.1.0_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 SI4091-8.2.1.0_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 3. 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 3. 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 315)
   - XModem Download (for details, see page 317)

   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 SI4091 10Gb System Interconnect Module 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 211. *General Maintenance Commands*

Command Syntax and Usage
copy flash-dump ftp [extm-port|mgt-port] Saves the system dump information via FTP. For details, see page 333. **Command mode:** All except User EXEC
copy flash-dump sftp [extm-port|mgt-port] Saves the system dump information via SFTP. For details, see page 333. **Command mode:** All except User EXEC
copy flash-dump tftp [address|extm-port| |filename|mgt-port] Saves the system dump information via TFTP. For details, see page 333. **Command mode:** All except User EXEC
clear flash-dump Clears dump information from flash memory. **Command mode:** All except User EXEC
copy log sftp [extm-port|mgt-port] Saves the system log file (SYSLOG) via SFTP. **Command mode:** All except User EXEC
copy log tftp [address|filename|mgt-port] Saves the system log file (SYSLOG) via TFTP. **Command mode:** All except User EXEC
copy sal sftp [extm-port|mgt-port] Saves the security audit log file via SFTP. **Command mode:** All except User EXEC

Table 211. *General Maintenance Commands*

Command Syntax and Usage
copy sal tftp [address|filename|mgt-port] Saves the security audit log file via TFTP. **Command mode:** All except User EXEC
clear sal Clears the security audit log file. **Command mode:** All except User EXEC
copy tech-support ftp [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 [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|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 SI4091 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 212. *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 *<LAG number>* Displays all FDB entries for a particular LAG. **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 212. *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 Network 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 213. *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 213. *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 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 Route Manipulation

The following table displays IP Route maintenance commands.

Table 214. *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 32 on page 63. **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 31 on page 63. **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 62.

LLDP Cache Manipulation

Table 215 describes the LLDP cache manipulation commands.

Table 215. *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 54. **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 216 describes the IGMP group maintenance commands.

Table 216. *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 *<LAG number>* Displays all IGMP multicast groups on a single LAG. **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 217. *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 *<LAG 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 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

IPv6 Neighbor Discovery Cache Manipulation

Table 218 describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 218. *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 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

IPv6 Route Maintenance

Table 219 describes the IPv6 route maintenance commands.

Table 219. *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

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:

```
SI 4091# copy flash-dump tftp [address|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:

```
SI 4091# copy flash-dump sftp [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:

```
SI 4091# copy flash-dump ftp [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:

```
SI 4091# 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.
```

Appendix A. Lenovo N/OS System Log Messages

The SI4091 10Gb System Interconnect Module (SI4091) 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!
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
MGMT	Maximum number of login failures (<*threshold*>) has been exceeded.
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>

LOG_CRIT

Thread	LOG_CRIT Message
AUDIT	NTP: cannot contact NTP server %s
AUDIT	NTP: System clock not updated. Authentication failed
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*>.
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	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
MGMT	/* Config changes at <*time*> by <*username*> */ <*config diff*> /* Done */
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*>

Thread	LOG_INFO Message (continued)
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
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()
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 EM|SCP|SNMP]
MGMT	new configuration saved from {ISCLI|SNMP}
MGMT	scp <*username*>(<*user type*>) {logout|ejected|idle timeout|connection closed} from {Console|Telnet/SSH}

Thread	LOG_INFO Message (continued)
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 SNMP]
MGMT	Unsupported GBIC {accepted|refused}
MGMT	Watchdog has been {enabled|disabled}
MGMT	Watchdog timeout interval is now <*seconds*> seconds)
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}

Thread	LOG_INFO Message (continued)
SSH	Wrong config file type
SYSTEM	booted version <*version*> from Flash image <*image*>, {active|backup|factory} config block

LOG_NOTICE

Thread	LOG_NOTICE Message
	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*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
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 {TELNET} from host <*IP address*>.
MGMT	Failed login attempt via the CONSOLE
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI

Thread	LOG_NOTICE Message (continued)
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper|operator} changed by {SNMP user|<*username*>}, notifying admin to save.
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	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	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
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

Thread	LOG_NOTICE Message (continued)
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*>
SYSTEM	rebooted (<*reason*>)[, administrator logged in] Reason: • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • • 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

LOG_WARNING

Thread	LOG_WARNING Message
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: 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	LDAP security does not meet security strict mode requirements
AUDIT	RADIUS security does not meet security strict mode requirements
AUDIT	TACACS+ security does not meet security strict mode requirements
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 - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC (until April 19, 2016) and EU Council Directive 2014/30/EU (from April 20, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A equipment according to European Standards harmonized in the Directives in compliance. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

CE Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Germany Class A Statement

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der Klasse A der Norm gemäß Richtlinie.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein

Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EU Richtlinie 2014/30/EU (früher 2004/108/EC), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahrenist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

Japan VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI–A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines (products less than or equal to 20 A per phase)

高調波ガイドライン準用品

Japan Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guidelines with Modifications (products greater than 20 A per phase).

Korea Communications Commission (KCC) Statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission Statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，
可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance Statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Index

Numerics

A

B

C

D

E

J

K

L

M

S

T

U

V

W

Lenovo

Part Number: 00MY393

Printed in USA

(IP) P/N: 00MY393