

Lenovo Flex System Fabric SI4093 System Interconnect Module

ISCLI—Industry Standard CLI Command Reference

For Lenovo Network Operating System 8.3

LenovoTM

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)

© Copyright Lenovo 2015

Portions © Copyright IBM Corporation 2014.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

Contents

Preface	11
Who Should Use This Book12
How This Book Is Organized13
Typographic Conventions14
Chapter 1. ISCLI Basics	17
ISCLI Command Modes18
Global Commands20
Command Line Interface Shortcuts22
CLI List and Range Inputs22
Command Abbreviation22
Tab Completion22
User Access Levels23
Idle Timeout24
Chapter 2. Information Commands.	25
System Information26
CLI Display Information27
Error Disable and Recovery Information28
SNMPv3 System Information29
SNMPv3 USM User Table Information30
SNMPv3 View Table Information31
SNMPv3 Access Table Information32
SNMPv3 Group Table Information.33
SNMPv3 Community Table Information33
SNMPv3 Target Address Table Information.34
SNMPv3 Target Parameters Table Information35
SNMPv3 Notify Table Information.36
SNMPv3 Dump Information37
General System Information38
Show Software Version Brief39
Show Recent Syslog Messages40
Show Security Audit Log Messages41
User Status42
Layer 2 Information.43
FDB Information44
Show All FDB Information45
Show FDB Multicast Address Information46
Clearing Entries from the Forwarding Database46
Link Aggregation Control Protocol Information.47
Link Aggregation Control Protocol47
Layer 2 Failover Information Commands.49
Layer 2 Failover Information49
Hot Links Information51
Edge Control Protocol Information52
LLDP Information.53
LLDP Remote Device Information54

Unidirectional Link Detection Information 55
UDLD Port Information 55
OAM Discovery Information 56
OAM Port Information. 56
LAG Information 57
VLAN Information 58
Layer 3 Information. 60
IPv6 Routing Information 62
IPv6 Routing Table 63
IPv6 Neighbor Discovery Cache Information 64
IPv6 Neighbor Discovery Cache Information 64
IGMP Information 65
IGMP Group Information 67
IGMP Multicast Router Information 68
IPMC Group Information 68
Interface Information 69
IPv6 Interface Information 70
IPv6 Path MTU Information 71
IP Information 72
Quality of Service Information 74
802.1p Information 75
WRED and ECN Information. 76
Access Control List Information Commands 77
Access Control List Information 78
RMON Information Commands 79
RMON History Information 80
RMON Alarm Information. 81
RMON Event Information 82
Link Status Information 83
Port Information 84
Port Transceiver Status 86
VM Ready Information 88
VMReady Information. 90
VM OUI Information 90
VM Port Information 91
VM Portchannel Information 91
VM Information 92
VM Check Information 92
VM Group Information 93
VM Bandwidth Information 93
VM Profile Information 93

VMware Information94
VMware Hello Information95
VMware Host Information95
VMware VM Information.97
ESX Server - Switchport Mapping97
EVB Information98
EVB VSIType Information99
EVB VMs Information	100
SLP Information	101
UFP Information	102
Port Information	103
CDCP Information	104
QoS Information	104
TLV Status Information	105
Virtual Port Information	106
VLAN Information	107
TLV Information	108
DCBX Information Commands	110
Converged Enhanced Ethernet Information	111
DCBX Information	112
DCBX Control Information	113
DCBX Feature Information	114
DCBX ETS Information	115
DCBX PFC Information	116
DCBX Application Protocol Information	117
ETS Information	119
PFC Information	120
FCoE Information.	121
FIP Snooping Information	121
Information Dump	123
Chapter 3. Statistics Commands.125
Forwarding Database Statistics	126
Port Statistics	127
Bridging Statistics	129
Ethernet Statistics	130
Interface Statistics	133
Interface Protocol Statistics	136
Link Statistics.	136
RMON Statistics	137
QoS Queue Statistics.	140
Link Aggregation Group (LAG) Statistics	144
Trunk Group Interface Statistics.	144
Layer 2 Statistics	145
LACP Statistics	146
Hotlinks Statistics	147
LLDP Port Statistics	148
OAM Statistics	149
Layer 3 Statistics	150
IPv4 Statistics.	152

IPv6 Statistics	155
IPv6 Route Statistics.	160
DNS Statistics	161
TCP Statistics.	161
UDP Statistics	163
IGMP Statistics	164
Management Processor Statistics	166
Packet Statistics.	167
MP Packet Statistics	167
Packet Statistics Log.	172
Packet Log example	172
Packet Statistics Last Packet	173
Packet Statistics Dump	173
Logged Packet Statistics	174
TCP Statistics.	177
UDP Statistics	178
CPU Statistics	178
CPU Statistics History	180
Access Control List Statistics	181
ACL Statistics	182
ACL Meter Statistics	182
VMAP Statistics	182
Fibre Channel over Ethernet Statistics	183
SNMP Statistics	184
NTP Statistics	188
SLP Statistics.	190
Statistics Dump	191
Chapter 4. Configuration Commands	193
Viewing and Saving Changes	194
Saving the Configuration	194
System Configuration.	195
System Error Disable and Recovery Configuration	199
Link Flap Dampening Configuration.	200
System Host Log Configuration.	201
SSH Server Configuration	204
RADIUS Server Configuration	206
TACACS+ Server Configuration	208
LDAP Server Configuration	212
NTP Server Configuration	214
NTP MD5 Key Commands	216
System SNMP Configuration.	217

SNMPv3 Configuration	219
User Security Model Configuration	221
SNMPv3 View Configuration	222
View-based Access Control Model Configuration	223
SNMPv3 Group Configuration	224
SNMPv3 Community Table Configuration	225
SNMPv3 Target Address Table Configuration	226
SNMPv3 Target Parameters Table Configuration	227
SNMPv3 Notify Table Configuration	228
System Access Configuration	229
Management Network Configuration	231
NETCONF Configuration	232
User Access Control Configuration	233
System User ID Configuration	234
Strong Password Configuration	235
Custom Daylight Saving Time Configuration	237
Port Configuration	238
Port Error Disable and Recovery Configuration	243
Port Link Configuration	244
Temporarily Disabling a Port	244
Unidirectional Link Detection Configuration	245
Port OAM Configuration	246
Port ACL Configuration	247
Port WRED Configuration	248
Port WRED Transmit Queue Configuration	249
Management Port Configuration	250
Quality of Service Configuration	251
802.1p Configuration	251
DSCP Configuration	252
Control Plane Protection	253
Weighted Random Early Detection Configuration	255
WRED Transmit Queue Configuration	255
Access Control Configuration	257
Access Control List Configuration	258
Ethernet Filtering Configuration	259
IPv4 Filtering Configuration	260
TCP/UDP Filtering Configuration	261
Packet Format Filtering Configuration	262
ACL IPv6 Configuration	263
IPv6 Filtering Configuration	264
IPv6 TCP/UDP Filtering Configuration	265
VMAP Configuration	266
ACL Group Configuration	271
ACL Metering Configuration	272
ACL Re-Mark Configuration	273
Re-Marking In-Profile Configuration	274
Re-Marking Out-Profile Configuration	274

IPv6 Re-Marking Configuration.	275
IPv6 Re-Marking In-Profile Configuration	276
IPv6 Re-Marking Out-Profile Configuration	276
Port Mirroring	277
Port Mirroring Configuration.	278
Layer 2 Configuration.	279
Forwarding Database Configuration.	279
Static Multicast MAC Configuration	280
Static FDB Configuration.	281
LLDP Configuration	282
LLDP Port Configuration.	283
LLDP Optional TLV configuration.	284
Link Aggregation Group (LAG) Configuration	286
Link Aggregation Group (LAG) Hash Configuration	288
FCoE LAG Hash Configuration	289
Layer 2 LAG Hash.	290
Layer 3 LAG Hash.	291
Link Aggregation Control Protocol Configuration.	292
LACP Port Configuration	293
Layer 2 Failover Configuration	295
Failover Trigger Configuration	296
Auto Monitor Configuration	296
Failover Manual Monitor Port Configuration	297
Failover Manual Monitor Control Configuration	298
Hot Links Configuration.	299
Hot Links Trigger Configuration	300
Hot Links Master Configuration.	301
Hot Links Backup Configuration	302
VLAN Configuration	303
Private VLAN Configuration	305
Layer 3 Configuration.	306
IP Interface Configuration	307
IPv6 Neighbor Discovery Configuration	308
Default Gateway Configuration.	311
Network Filter Configuration.	312
IGMP Configuration	313
IGMP Snooping Configuration	314
IGMPv3 Configuration.	315
IGMP Filtering Configuration.	316
IGMP Static Multicast Router Configuration	318
IGMP Advanced Configuration	319
Domain Name System Configuration	320
IPv6 Default Gateway Configuration	321
IPv6 Path MTU Configuration	322
Converged Enhanced Ethernet Configuration	323
ETS Global Configuration	324
ETS Global Priority Group Configuration.	324
Priority Flow Control Configuration.	325
Global Priority Flow Control Configuration.	325
Port-level 802.1p PFC Configuration	326

DCBX Port Configuration	327
Fibre Channel over Ethernet Configuration.	328
FIPS Port Configuration	329
Remote Monitoring Configuration	330
RMON History Configuration	330
RMON Event Configuration	331
RMON Alarm Configuration	332
VMReady	334
VM Policy Bandwidth Management	335
VM Group Configuration	336
VM Check Configuration.	339
VM Profile Configuration	340
VMWare Configuration	341
Miscellaneous VMready Configuration	342
UFP Configuration	343
Edge Virtual Bridge Configuration	346
Edge Virtual Bridge Profile Configuration	348
Switch Partition (SPAR) Configuration	349
Service Location Protocol Configuration	351
Configuration Dump	352
Saving the Active Switch Configuration	353
Restoring the Active Switch Configuration	354
Chapter 5. Operations Commands	355
Operations-Level Port Commands	356
Protected Mode Options	357
VMware Operations	359
VMware Distributed Virtual Switch Operations	361
VMware Distributed Port Group Operations	362
Edge Virtual Bridge Operations.	363
Feature on Demand Key Options	364
Chapter 6. Boot Options	367
Scheduled Reboot.	368
Netboot Configuration	369
Flexible Port Mapping.	370
QSFP Port Configuration	371
Updating the Switch Software Image	372
Loading New Software to Your Switch.	372
Selecting a Software Image to Run.	373
Uploading a Software Image from Your Switch	373
Selecting a Configuration Block.	375
Rebooting the Switch	376
Using the Boot Management Menu	377
Boot Recovery Mode	378
Recover from a Failed Image Upgrade using TFTP.	379
Recovering from a Failed Image Upgrade using XModem Download	381
Physical Presence	383

Chapter 7. Maintenance Commands	385
Forwarding Database Maintenance	387
Debugging Commands	389
LLDP Cache Manipulation.	391
IGMP Group Maintenance.	392
IGMP Multicast Routers Maintenance	393
IPv6 Neighbor Discovery Cache Manipulation	394
IPv6 Route Maintenance.	395
TFTP, SFTP or FTP System Dump Copy	396
Clearing Dump Information	397
Appendix A. Lenovo N/OS System Log Messages	399
LOG_ALERT	400
LOG_CRIT	401
LOG_ERR	402
LOG_INFO	404
LOG_NOTICE	408
LOG_WARNING	412
Appendix B. Getting help and technical assistance.	415
Appendix C. Notices	417
Trademarks	419
Important Notes	420
Recycling Information.	421
Particulate Contamination.	422
Telecommunication Regulatory Statement	423
Electronic Emission Notices	424
Federal Communications Commission (FCC) Statement	424
Industry Canada Class A Emission Compliance Statement	424
Avis de Conformité à la Réglementation d'Industrie Canada	424
Australia and New Zealand Class A Statement	424
European Union - Compliance to the Electromagnetic Compatibility Directive	425
Germany Class A Statement	425
Japan VCCI Class A Statement	426
Japan Electronics and Information Technology Industries Association	
(JEITA) Statement	427
Korea Communications Commission (KCC) Statement	427
Russia Electromagnetic Interference (EMI) Class A Statement	427
People's Republic of China Class A electronic emission Statement	427
Taiwan Class A compliance Statement	427
Index	429

Preface

The *Lenovo Flex System Fabric SI4093 System Interconnect Module ISCLI Command Reference* describes how to configure and use the Lenovo N/OS 8.3 software with your Lenovo Flex System Fabric SI4093 System Interconnect Module (referred to as SI4093 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 SI4093. For details about the configuration and operation of the SI4093, 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, or 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 <code>readme.txt</code> 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.
<i>italicized body text</i>	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 []	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is show interface ip [<125-128>]</p> <p>you enter show interface ip</p> <p>or show interface ip <125-128></p>
vertical line	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is show portchannel {<1-128> hash information}</p> <p>you must enter: show portchannel <1-128></p> <p>or show portchannel hash</p> <p>or show portchannel information</p>

Chapter 1. ISCLI Basics

Your SI4093 System Interconnect Module (SI4093) 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 SI4093.

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 SI4093. 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 4093>	Default mode, entered automatically on console Exit: exit or logout
Privileged EXEC SI 4093#	Enter Privileged EXEC mode, from User EXEC mode: enable Exit to User EXEC mode: disable Quit ISCLI: exit or logout
Global Configuration SI 4093(config)#	Enter Global Configuration mode, from Privileged EXEC mode: configure terminal Exit to Privileged EXEC: end or exit
Interface IP SI 4093(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 4093(config-if)#	Enter Port Configuration mode, from Global Configuration mode: interface port <port number or alias> Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end
Interface PortChannel SI 4093(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 4093(config-vlan)#	Enter VLAN Configuration mode, from Global Configuration mode: vlan <VLAN number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
VSI Database SI 4093(conf-vsldb)#	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: virt evb vsldb <VSIDB_number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
EVB Profile SI 4093(conf-evbprof)#	Enter Edge Virtual Bridging Profile Configuration mode, from Global Configuration mode: virt evb profile <1-16> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
UFP Virtual Port Configuration SI 4093(config_ufp_vport)#	Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: ufp port <port no.> vport <1-4> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
SPAR Configuration SI 4093(config-spar)#	Enter Switch Partition Configuration mode, from Global Configuration mode: spar <1-8> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end

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
<code>?</code>	Provides more information about a specific command or lists commands available at the current level.
<code>list</code>	Lists the commands available at the current level.
<code>exit</code>	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
<code>copy running-config startup-config</code>	Write configuration changes to non-volatile flash memory.
<code>logout</code>	Exit from the command line interface and log out.
<code>ping</code>	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>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]</pre> <p>Where:</p> <ul style="list-style-type: none"> 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 <i>don't fragment</i> bit in the IP header (only for IPv4 addresses). o -t: Pings continuously (same as -n 0). <p>Where the <i>IP address</i> or <i>hostname</i> specify the target device. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Tries</i> (optional) is the number of attempts (1-32), and <i>msec delay</i> (optional) is the number of milliseconds between attempts.</p>

Table 2. Description of Global Commands (continued)

Command	Action
tracert	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <p>tracert {<hostname> <IP address>} [<max-hops (1-32)> [<msec-delay (1-4294967295)>]]</p> <p>Where <i>hostname/IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-32 devices), and <i>msec-delay</i> (optional) is the number of milliseconds to wait for the response.</p> <p>As with ping, the DNS parameters must be configured if specifying hostnames.</p>
telnet	<p>This command is used to form a Telnet session between the switch and another network device. The format is as follows:</p> <p>telnet {<hostname> <IP address>} [<port>]</p> <p>Where <i>IP address</i> or <i>hostname</i> specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch.</p> <p><i>Port</i> is the logical Telnet port or service number.</p>
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 4093(config)# vlan 1,3,4095	(access VLANs 1, 3, and 4095)
SI 4093(config)# vlan 1-20	(access VLANs 1 through 20)
SI 4093(config)# vlan 1-5,90-99,4090-4095	(access multiple ranges)
SI 4093(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 4093(config)# interface port 1-4	(access ports 1 through 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 4093(config)# show mac-address-table interface port 12
--

or:

SI 4093(config)# sh ma i p 12

Tab Completion

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

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the SI4093. 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 SI4093. 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 SI4093. 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 SI4093. 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 SI4093, 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
<p>show interface status <i><port alias or number></i></p> <p>Displays configuration information about the selected port(s), including:</p> <ul style="list-style-type: none">o Port alias and numbero Port speedo Duplex mode (half, full, or auto)o Flow control for transmit and receive (no, yes, or both)o Link status (up, down, or disabled) <p>For details, see page 83.</p> <p>Command mode: All</p>
<p>show interface trunk <i><port alias or number></i></p> <p>Displays port status information, including:</p> <ul style="list-style-type: none">o Port alias and numbero Whether the port uses VLAN Tagging or noto Port VLAN ID (PVID)o Port nameo VLAN membershipo FDB Learning statuso Flooding status <p>For details, see page 84.</p> <p>Command mode: All</p>
<p>show interface transceiver</p> <p>Displays the status of the port transceiver module on each external port. For details, see page 86.</p> <p>Command mode: All</p>
<p>show information-dump</p> <p>Dumps all switch information available (10K or more, depending on your configuration).</p> <p>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.</p> <p>Command mode: All</p>

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
<p>show sys-info</p> <p>Displays system information, including:</p> <ul style="list-style-type: none">o System date and timeo Switch model name and numbero Switch name and locationo Time of last booto MAC address of the switch management processoro IP address of management interfaceo Hardware version and part numbero Software image file and version numbero Configuration nameo Log-in banner, if one is configuredo Internal temperatures <p>For details, see page 38.</p> <p>Command mode: All</p>
<p>show logging [severity <0-7>] [reverse]</p> <p>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.</p> <p>Command mode: All</p>
<p>show access user</p> <p>Displays configured user names and their status.</p> <p>Command mode: Privileged EXEC</p>

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 195 . Command mode: All
show line vty length Displays the current line vty length setting. For details, see page 195 . 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
<p>show snmp-server v3 notify</p> <p>Displays the Notify table information. To view a sample, see page 36.</p> <p>Command mode: All</p>
<p>show snmp-server v3</p> <p>Displays all the SNMPv3 information. To view a sample, see page 37.</p> <p>Command mode: All</p>

SNMPv3 USM User Table Information

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

show snmp-server v3 user

Command mode: All

The USM user table contains the following information:

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

usmUser Table:	
User Name	Protocol

adminmd5	HMAC_MD5, DES PRIVACY
adminsha	HMAC_SHA, DES PRIVACY
v1v2only	NO AUTH, NO PRIVACY

Table 9. *USM User Table Information Parameters*

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. Lenovo N/OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table Information

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

The following command displays the SNMPv3 View Table:

```
show snmp-server v3 view
```

Command mode: All

View Name	Subtree	Mask	Type
iso	1		included
v1v2only	1		included
v1v2only	1.3.6.1.6.3.15		excluded
v1v2only	1.3.6.1.6.3.16		excluded
v1v2only	1.3.6.1.6.3.18		excluded

Table 10. *SNMPv3 View Table Information Parameters*

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

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

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

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

The following command displays SNMPv3 access information:

```
show snmp-server v3 access
```

Command mode: All

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

Table 11. *SNMPv3 Access Table Information*

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

SNMPv3 Group Table Information

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

The following command displays SNMPv3 group information:

show snmp-server v3 group

Command mode: All

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

Table 12. *SNMPv3 Group Table Information Parameters*

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

SNMPv3 Community Table Information

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

show snmp-server v3 community

Command mode: All

Index	Name	User Name	Tag
trap1	public	v1v2only	v1v2trap

Table 13. *SNMPv3 Community Table Information Parameters*

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

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

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

Command mode: All

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

Name	Transport Addr	Port	Taglist	Params
trap1	47.81.25.66	162	v1v2trap	v1v2param

Table 14. *SNMPv3 Target Address Table Information Parameters*

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

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

show snmp-server v3 target-parameters

Command mode: All

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

Table 15. *SNMPv3 Target Parameters Table Information*

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

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify table:

```
show snmp-server v3 notify
```

Command mode: All

Name	Tag
v1v2trap	v1v2trap

Table 16. *SNMPv3 Notify Table Information*

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

show snmp-server v3

Command mode: All

```

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

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

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

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

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

snmpNotify Table:
Name Tag
-----

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

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

```

General System Information

The following command displays system information:

show sys-info

Command mode: All

```
System Information at 15:20:43 Wed Jan 28, 2015
Time zone: No timezone configured
Daylight Savings Time Status: Disabled

Lenovo Flex System Fabric SI4093 System Interconnect Module

Switch has been up for 0 days, 0 hours, 27 minutes and 3 seconds.
Last boot: 14:55:53 Wed Jan 28, 2015 (reset from console)

MAC address: a8:97:dc:7f:15:00
Internal Management Port MAC Address: a8:97:dc:7f:15:ef
Internal Management Port IP Address (if 128): 192.168.70.120
External Management Port MAC Address: a8:97:dc:7f:15:fe
External Management Port IP Address (if 127): 10.241.10.50

Software Version 7.9.1 (FLASH image2), active configuration.
Boot kernel version 7.9.1

Hardware Part Number      : 95Y3315
Hardware Revision         : 05
Serial Number             : Y011CM3BB008
Manufacturing Date (WWYY) : 4713
PCBA Part Number         : 00D6224
PCBA Revision            : 0
PCBA Number              : 00
Board Revision           : 05
PLD Firmware Version     : 1.7

Temperature Warning       : 34 C (Warning at 66 C / Recover at 61 C)
Temperature Shutdown     : 34 C (Shutdown at 72 C / Recover at 67 C)
Temperature Inlet        : 29 C
Temperature Exhaust      : 34 C
Temperature Asic Max     : 35 C (Warning at 100 C / Shutdown at 108 C)

Power Consumption        : 34.110 W (12.220 V  2.789 A)

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

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

System information includes:

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

Show Software Version Brief

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

Table 17. *Specific System Information Options*

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

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

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

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

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

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

Date      Time      Criticality level      Message
Jul  8  17:25:41    NOTICE      system: link up on port INT1
Jul  8  17:25:41    NOTICE      system: link up on port INT8
Jul  8  17:25:41    NOTICE      system: link up on port INT7
Jul  8  17:25:41    NOTICE      system: link up on port INT2
Jul  8  17:25:41    NOTICE      system: link up on port INT1
Jul  8  17:25:41    NOTICE      system: link up on port INT4
Jul  8  17:25:41    NOTICE      system: link up on port INT3
Jul  8  17:25:41    NOTICE      system: link up on port INT6
Jul  8  17:25:41    NOTICE      system: link up on port INT5
Jul  8  17:25:41    NOTICE      system: link up on port EXT4
Jul  8  17:25:41    NOTICE      system: link up on port EXT1
Jul  8  17:25:41    NOTICE      system: link up on port EXT3
Jul  8  17:25:41    NOTICE      system: link up on port EXT2
Jul  8  17:25:41    NOTICE      system: link up on port INT3
Jul  8  17:25:42    NOTICE      system: link up on port INT2
Jul  8  17:25:42    NOTICE      system: link up on port INT4
Jul  8  17:25:42    NOTICE      system: link up on port INT3
Jul  8  17:25:42    NOTICE      system: link up on port INT6
```

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

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

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

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

Show Security Audit Log Messages

The following commands display security audit log messages:

Table 18. *Security Audit Log Information Commands*

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

Command sample output for `show sal`:

<pre>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</pre>
<pre>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</pre>
<pre>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</pre>
<pre>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</pre>

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
<p>show portchannel information</p> <p>Displays the state of each port in the various Link Aggregation Groups (LAGs). For details, see page 57.</p> <p>Command mode: All</p>
<p>show vlan</p> <p>Displays VLAN configuration information for all configured VLANs, including:</p> <ul style="list-style-type: none">o VLAN Numbero VLAN Nameo Statuso Port membership of the VLAN <p>For details, see page 58.</p> <p>Command mode: All</p>
<p>show failover trigger [<i><trigger number></i>]information</p> <p>Displays Layer 2 Failover information. For details, see page 49.</p> <p>Command mode: All</p>
<p>show hotlinks information</p> <p>Displays Hot Links information. For details, see page 51.</p> <p>Command mode: All</p>
<p>show layer2 information</p> <p>Dumps all Layer 2 switch information available (10K or more, depending on your configuration).</p> <p>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.</p> <p>Command mode: All</p>

FDB Information

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

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

Table 20. *FDB Information Commands*

Command Syntax and Usage
<p>show mac-address-table</p> <p>Displays all entries in the Forwarding Database.</p> <p>Command mode: All</p> <p>For more information, see page 45.</p>
<p>show mac-address-table address <MAC address></p> <p>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.</p> <p>You can also enter the MAC address using the format, xxxxxxxxxxxx. For example, 080020123456.</p> <p>Command mode: All</p>
<p>show mac-address-table all</p> <p>Displays both unicast (static and dynamic) and multicast (static) entries in the Forwarding Database.</p> <p>Command mode: All</p>
<p>show mac-address-table configured static</p> <p>Displays all configured static MAC entries in the FDB.</p> <p>Command mode: All</p>
<p>show mac-address-table interface port <port alias or number></p> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All</p>
<p>show mac-address-table multicast</p> <p>Displays all Multicast MAC entries in the FDB.</p> <p>Command mode: All</p>
<p>show mac-address-table portchannel <LAG number></p> <p>Displays all FDB entries for a particular Link Aggregation Group (LAG).</p> <p>Command mode: All</p>
<p>show mac-address-table private-vlan <VLAN number></p> <p>Displays all FDB entries on a single private VLAN.</p> <p>Command mode: All</p>

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 387](#).

Link Aggregation Control Protocol Information

Use these commands to display LACP status information about each port on the SI4093.

Table 22. *LACP Information Commands*

Command Syntax and Usage
<p>show lacp aggregator <aggregator ID></p> <p>Displays detailed information about the LACP aggregator.</p> <p>Command mode: All</p>
<p>show lacp information</p> <p>Displays a summary of LACP information. For details, see page 47.</p> <p>Command mode: All</p>
<p>show interface port <port alias or number> lacp information</p> <p>Displays LACP information about the selected port.</p> <p>Command mode: All</p>

Link Aggregation Control Protocol

The following command displays LACP information:

show lacp information

Command mode: All

port	mode	adminkey	operkey	selected	prio	aggr	trunk	status	minlinks
INTA1	off	1	1	no	32768	--	--	--	1
INTA2	off	2	2	no	32768	--	--	--	1
INTA3	off	3	3	no	32768	--	--	--	1
INTA4	off	4	4	no	32768	--	--	--	1
INTA5	off	5	5	no	32768	--	--	--	1
INTA6	off	6	6	no	32768	--	--	--	1
INTA7	off	7	7	no	32768	--	--	--	1
INTA8	off	8	8	no	32768	--	--	--	1
INTA9	off	9	9	no	32768	--	--	--	1
INTA10	off	10	10	no	32768	--	--	--	1
INTA11	off	11	11	no	32768	--	--	--	1
INTA12	off	12	12	no	32768	--	--	--	1
INTA13	off	13	13	no	32768	--	--	--	1
INTA14	off	14	14	no	32768	--	--	--	1
EXT1	active	1000	1000	no	32768	--	65*	down	1
EXT2	active	1000	1000	no	32768	--	65*	down	1
EXT3	active	1000	1000	no	32768	--	65*	down	1
EXT4	active	1000	1000	no	32768	--	65*	down	1
EXT5	active	1000	1000	no	32768	--	65*	down	1
EXT6	active	1000	1000	no	32768	--	65*	down	1
EXT7	active	1000	1000	no	32768	--	65*	down	1
EXT8	active	1000	1000	no	32768	--	65*	down	1
EXT9	active	1000	1000	no	32768	--	65*	down	1
EXT10	active	1000	1000	no	32768	--	65*	down	1

(*) LACP PortChannel is statically bound to the admin key

LACP dump includes the following information for each external port in the SI4093:

- **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 (UFP feature is not enabled in switch, port is not configured as UFP port, vport is not enabled or physical port is not enabled).

Hot Links Information

The following command displays Hot Links information:

show hotlinks information

Command mode: All

```
Hot Links Info: Trigger

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

Current Trigger 12 setting: enabled
name "TG-12", preempt enabled, fdelay 30 sec, 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 port <1-16> tlv evb Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information. Command mode: All
show lldp port <1-16> vport <1-4> tlv evb Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information for the specific virtual port. Command mode: All
show lldp receive Displays information about the LLDP receive state machine. Command mode: All
show lldp remote-device [<1-256> detail port [<port number or range>]] Displays information received from LLDP-capable devices. To view a sample display, see page 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 <code>type</code> option lists only the VLAN type for each private VLAN: <code>community</code> , <code>isolated</code> or <code>primary</code> . Command mode: All
show vlan information Displays information about all VLANs, including: <ul style="list-style-type: none">o VLAN number and nameo Port membershipo VLAN status (enabled or disabled)o Private VLAN statuso Virtual ports 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	empty
4081	SPAR 1 (DVLAN)	ena	dis	INTA1-INTA14 EXT1-EXT10
4091	Black-hole VLAN	ena	dis	empty
4095	Mgmt VLAN	ena	ena	EXTM MGT1

Primary	Secondary	Type	Ports	vPorts
-----	-----	-----	-----	-----

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 69 . 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 65 . Command mode: All
show ip information Displays all IP information. Command mode: All
show ip interface brief Displays IP Information. For details, see page 72 . IP information, includes: <ul style="list-style-type: none">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 slp Displays information about the Service Location Protocol (SLP) configuration. For command options, see page 101 . Command mode: All
show ipv6 gateway6 <3-4> Displays the current IPv6 default gateway configuration. Command mode: All

Table 29. Layer 3 Information Commands (continued)

Command Syntax and Usage
<p>show ipv6 interface [<i><interface number></i>]</p> <p>Displays IPv6 interface information. For details, see page 70.</p> <p>Command mode: All</p>
<p>show ipv6 neighbors</p> <p>Displays IPv6 Neighbor Discovery cache information. For more information options, see page 64.</p> <p>Command mode: All</p>
<p>show ipv6 pmtu [<i><destination IPv6 address></i>]</p> <p>Displays IPv6 Path MTU information. For details, see page 71.</p> <p>Command mode: All</p>
<p>show layer3</p> <p>Dumps all Layer 3 switch information available (10K or more, depending on your configuration).</p> <p>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.</p> <p>Command mode: All</p>

IPv6 Routing Information

Table 30 describes the IPv6 Routing information options.

Table 30. *IPv6 Routing Information Commands*

Command Syntax and Usage
show ipv6 route Displays all IPv6 routing information. For more information, see page 63 . Command mode: All
show ipv6 route address <IPv6 address> Displays a single route by destination IP address. Command mode: All
show ipv6 route gateway <default gateway address> Displays routes to a single gateway. Command mode: All
show ipv6 route interface <interface number> Displays routes on a single interface. Command mode: All
show ipv6 route static Displays all static IPv6 routes. Command mode: All
show ipv6 route type {connected static ospf} Displays routes of a single type. Command mode: All
show ipv6 route summary Displays a summary of IPv6 routing information, including inactive routes. Command mode: All

IPv6 Routing Table

The following command displays IPv6 routing information:

show ipv6 route

Command mode: All

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

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

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

IPv6 Neighbor Discovery Cache Information

The following commands display IPv6 Neighbor Discovery Cache information.

Table 31. *IPv6 Neighbor Discovery Cache Information Commands*

Command Syntax and Usage
<p>show ipv6 neighbors</p> <p>Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 64.</p> <p>Command mode: All</p>
<p>show ipv6 neighbors find <IPv6 address></p> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address.</p> <p>Command mode: All</p>
<p>show ipv6 neighbors interface port <port alias or number></p> <p>Shows IPv6 Neighbor Discovery cache entries on a single port.</p> <p>Command mode: All</p>
<p>show ipv6 neighbors static</p> <p>Displays static IPv6 Neighbor Discovery cache entries.</p> <p>Command mode: All</p>
<p>show ipv6 neighbors vlan <VLAN number></p> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN.</p> <p>Command mode: All</p>

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 32. *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 67 . 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 68 . Command mode: All

Table 32. *IGMP Information Commands (continued)*

Command Syntax and Usage
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 mroouters: 2
Total number of installed static mroouters: 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
0 - 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

```
IP information:
  AS number 0

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:

Default gateway information: metric strict
3: 10.241.10.1, up active

Default IP6 gateway information:

ECMP Hash Mechanism: dipsip

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

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

Current network filter settings:
  none

Current route map settings:
  none

RIP is disabled.

OSPF is disabled.

Current OSPFv3 settings:
OSPFv3 is disabled.

Current PIM settings: OFF

BGP is disabled.
```


IP information includes:

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

Quality of Service Information

The following commands display Quality of Service information.

Table 33. *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 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 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 75 . Command mode: All
show qos random-detect Displays WRED ECN information. Command mode: All

802.1p Information

The following command displays 802.1p information:

show qos transmit-queue information

Command mode: All

```

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

Current port priority information:
Port     Priority  COSq  Weight
-----  -
INT1     0         0     1
INT2     0         0     1
...
MGT1     0         0     1
MGT2     0         0     1
EXT1     0         0     1
EXT2     0         0     1
EXT3     0         0     1
EXT4     0         0     1
...

```

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

Table 34. *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 35. *802.1p Port Priority Parameter Descriptions*

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

WRED and ECN Information

The following command displays WRED and ECN information:

show qos random-detect

Command mode: All

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

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

Access Control List Information Commands

The following commands display Access Control List information.

Table 36. *ACL Information Options*

Command Syntax and Usage
show access-control group [<i><1-256></i>] Displays ACL group information. Command mode: All
show access-control list [<i><1-256></i>] Displays ACL list information. For details, see page 78 . Command mode: All
show access-control list6 [<i><1-128></i>] Displays IPv6 ACL list information. Command mode: All
show access-control vmap [<i><1-128></i>] Displays VMAP information. Command mode: All

Access Control List Information

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

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

Command mode: All

```
Current ACL information:
-----
Filter 2 profile:
Ethernet
  - VID          : 2/0xffff
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 37. *ACL Parameter Descriptions*

Parameter	Description
Filter <i>x</i> 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 38. *RMON Information commands*

Command Syntax and Usage
show rmon Displays all RMON information. Command mode: All
show rmon alarm [<i><alarm group number></i>] Displays RMON Alarm information. For details, see page 81 . Command mode: All
show rmon event [<i><event group number></i>] Displays RMON Event information. For details, see page 82 . Command mode: All
show rmon history [<i><history group number></i>] Displays RMON History information. For details, see page 80 . 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 39. *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 40. 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 40. *RMON Alarm Parameter Descriptions (continued)*

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

RMON Event Information

The following command displays RMON Alarm information:

show rmon event

Command mode: All

```

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

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

The following table describes the RMON Event Information parameters.

Table 41. *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	-----	-----
INTA1	1	1G/10G	full	no	no	disabled	INTA1
INTA2	2	1G/10G	full	no	no	disabled	INTA2
INTA3	3	1G/10G	full	no	no	disabled	INTA3
INTA4	4	1G/10G	full	no	no	disabled	INTA4
INTA5	5	1G/10G	full	no	no	disabled	INTA5
INTA6	6	1G/10G	full	no	no	disabled	INTA6
INTA7	7	1G/10G	full	no	no	disabled	INTA7
INTA8	8	1G/10G	full	no	no	disabled	INTA8
INTA9	9	1G/10G	full	no	no	disabled	INTA9
INTA10	10	1G/10G	full	no	no	disabled	INTA10
INTA11	11	1G/10G	full	no	no	disabled	INTA11
INTA12	12	1G/10G	full	no	no	disabled	INTA12
INTA13	13	1G/10G	full	no	no	disabled	INTA13
INTA14	14	1G/10G	full	no	no	disabled	INTA14
EXT1	43	1G/10G	full	no	no	down	EXT1
EXT2	44	1G/10G	full	no	no	down	EXT2
EXT3	45	1G/10G	full	no	no	down	EXT3
EXT4	46	1G/10G	full	no	no	down	EXT4
EXT5	47	1G/10G	full	no	no	down	EXT5
EXT6	48	1G/10G	full	no	no	down	EXT6
EXT7	49	1G/10G	full	no	no	down	EXT7
EXT8	50	1G/10G	full	no	no	down	EXT8
EXT9	51	1G/10G	full	no	no	down	EXT9
EXT10	52	1G/10G	full	no	no	down	EXT10
EXTM	65	1000	full	yes	yes	up	EXTM
MGT1	66	1000	full	no	no	up	MGT1

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

Use this command to display link status information about each port on the SI4093, 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	Ln	Fld	PVID	DESCRIPTION	VLAN(s)
		Trk				NVLAN		
EXT3	45	n	d	e	e	4081#	EXT3	4081
EXT4	46	n	d	e	e	4081#	EXT4	4081
EXT5	47	n	d	e	e	4081#	EXT5	4081
EXT6	48	n	d	e	e	4081#	EXT6	4081
EXT7	49	n	d	e	e	4081#	EXT7	4081
EXT8	50	n	d	e	e	4081#	EXT8	4081
EXT9	51	n	d	e	e	4081#	EXT9	4081
EXT10	52	n	d	e	e	4081#	EXT10	4081
EXT11	53	n	d	e	e	4083#	EXT11	4083
EXT12	54	n	d	e	e	4083#	EXT12	4083
EXT13	55	n	d	e	e	4083#	EXT13	4083
EXT14	56	n	d	e	e	4083#	EXT14	4083
EXT15	57	n	d	e	e	4082#	EXT15	4082
EXT16	58	n	d	e	e	4082#	EXT16	4082
EXT17	59	n	d	e	e	4082#	EXT17	4082
EXT18	60	n	d	e	e	4082#	EXT18	4082
EXT19	61	n	d	e	e	4082#	EXT19	4082
EXT20	62	n	d	e	e	4082#	EXT20	4082
EXT21	63	n	d	e	e	4082#	EXT21	4082
EXT22	64	n	d	e	e	4082#	EXT22	4082
EXTM	65	n	d	e	e	4095	EXTM	4095
MGT1	66	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
49 EXT21	Down	SX SFP	Blade Network	BN-CKM-S-SX	Approved
50 EXT22	LINK	3m DAC	Blade Network	BN-SP-CBL-3M	Accepted
51 EXT23	LINK	SR SFP+	Blade Network	BN-CKM-SP-SR	Approved
52 EXT24	LINK	SR SFP+	Blade Network	BN-CKM-SP-SR	Approved

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 42. *Expected Transceiver Optical Power Levels*

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

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

VM Ready Information

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

Table 43. *Virtual Machines Information Options*

Command Syntax and Usage
<p>show virt</p> <p>Displays the current virtualization parameters. For a sample output, see page 90.</p> <p>Command mode: All</p>
<p>show virt oui</p> <p>Displays all the configured MAC OUIs. For a sample output, see page 90.</p> <p>Command mode: All</p>
<p>show virt port <port alias or number></p> <p>Displays VM Ready information for the selected port. For a sample output, see page 91.</p> <p>Command mode: All</p>
<p>show virt portchannel <portchannel group member></p> <p>Displays Virtual Machine information for the selected portchannel. For a sample output, see page 91.</p> <p>Command mode: All</p>
<p>show virt vm -v</p> <p>Displays all VM Ready information.</p> <ul style="list-style-type: none">o -v displays verbose information <p>For a sample output, see page 92.</p> <p>Command mode: All</p>
<p>show virt vmcheck</p> <p>Displays the current VM Check settings. For a sample output, see page 92.</p> <p>Command mode: All</p>
<p>show virt vmgroup [<1-4096>]</p> <p>Displays the current VM Group parameters. For a sample output, see page 93.</p> <p>Command mode: All</p>

Table 43. *Virtual Machines Information Options*

Command Syntax and Usage
<p>show virt</p> <p>Displays the current virtualization parameters. For a sample output, see page 90.</p> <p>Command mode: All</p>
<p>show virt oui</p> <p>Displays all the configured MAC OUIs. For a sample output, see page 90.</p> <p>Command mode: All</p>
<p>show virt vmpolicy vmbandwidth [<MAC address> <UUID> <name> <IP address> <index number>]</p> <p>Displays the current VM bandwidth management parameters. For a sample output, see page 93.</p> <p>Command mode: All</p>
<p>show virt vmprofile [<profile name>]</p> <p>Displays the current VM Profile parameters. For a sample output, see page 93.</p> <p>Command mode: All</p>

VMReady Information

The following command displays the current virtualization options:

show virt

Command mode: All

```
VMready is currently enabled

Current Hello setting: disabled

Current VMware-specific settings
-----

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

Current VM profiles:
-----
      None

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

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

VM OUI Information

The following command displays all the configured MAC OUIs:

show virt oui

Command mode: All

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

      Number of MAC OUI entries: 9
```

VM Port Information

The following command displays VM information for a specific port:

```
show virt port <port alias or number>
```

Command mode: All

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

Number of entries: 2

VM Portchannel Information

The following command displays VM information for a specific portchannel:

```
show virt portchannel <1-128>
```

Command mode: All

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

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

VM Information

The following command displays VM information:

```
show virt vm
```

Command mode: All

IP Address	VMAC Address	Index	Port	VM Group(Profile)	Check Status
*127.31.46.50	00:50:56:4e:62:f5	4	INTA3		
*127.31.46.10	00:50:56:4f:f2:85	2	INTA4		
+127.31.46.51	00:50:56:72:ec:86	1	INTA3		
+127.31.46.11	00:50:56:7c:1c:ca	3	INTA4		
127.31.46.25	00:50:56:9c:00:c8	5	INTA4		
127.31.46.15	00:50:56:9c:21:2f	0	INTA4		
127.31.46.35	00:50:56:9c:29:29	6	INTA3		

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

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

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

VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

Command mode: All

Action to take for spoofed VMs: Basic: Oper disable the link Advanced: Install ACL to drop traffic
Maximum number of acls that can be used for mac spoofing: 50
Trusted ports by configuration: empty

VM Group Information

The following command displays VM Group parameters:

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

Command mode: All

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

VM Bandwidth Information

The following command displays VM bandwidth management parameters:

```
show virt vmpolicy vmbwidth
```

Command mode: All

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

VM Profile Information

The following command displays VM Profile parameters:

```
show virt vmprofile
```

Command mode: All

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

VMware Information

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

Table 44. *VMware Information Options*

Command Syntax and Usage
show virt vmware hosts Displays a list of VMware hosts. For a sample output, see page 100 . Command mode: All
show virt vmware hello Displays VMware hello settings. For a sample output, see page 99 . Command mode: All
show virt vmware showhost {<host UUID> <host IP address> <host name>} Displays detailed information about a specific VMware host. For a sample output, see page 100 . Command mode: All
show virt vmware showvm {<VM UUID> <VM IP address> <VM name>} Displays detailed information about a specific Virtual Machine (VM). For a sample output, see page 97 . Command mode: All
show virt vmware switchport-mapping Displays ESX Server - switchport mapping. For a sample output, see page 97 . Command mode: All
show virt vmware vms Displays a list of VMs. For a sample output, see page 97 . Command mode: All

VMware Hello Information

The following command displays VM hello parameters:

```
show virt vmware hello
```

Command mode: All

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

VMware Host Information

The following command displays VM host information:

```
show virt vmware hosts
```

Command mode: All

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

VM host information includes the following:

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

The following command displays information for a specific VM host:

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

Command mode: All

```
Vswitches available on the host:

    vSwitch0
    vSwitch1

Host physical nics:

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

Port Groups and their vSwitches on the host:

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

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

```


VMware VM Information

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

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

Command mode: All

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

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

```
show virt vmware vms
```

Command mode: All

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

VMware VM information includes the following:

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

ESX Server - Switchport Mapping

The following command displays ESX Server - switchport mapping:

```
show virt vmware switchport-mapping
```

Command mode: All

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

EVB Information

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

Table 45. *EVB Information Options*

Command Syntax and Usage
show virt evb profile [ports] Displays all EVB profile parameters. The <code>ports</code> option also display port parameters. Command mode: All
show virt evb profile <1-16> [ports] Displays the selected EVB profile parameters. The <code>ports</code> option also display port parameters. Command mode: All
show virt evb vdp vm Displays all active Virtual Machines (VMs). For a sample output, see page 100 . Command mode: All
show virt evb vdp tlv Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs). Command mode: All
show virt evb vsidb <VSI_database_number> Displays Virtual Station Interface database information. Command mode: All
show virt evb vsitypes [mgrid <0-255> typeid <1-16777215> version <0-255>] Displays the current Virtual Station Interface Type database parameters. For a sample output, see page 99 . Command mode: All

EVB VSIType Information

The following command displays VSITypes database parameters:

```
show virt evb vsitypes
```

Command mode: All

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

```
Total number of VSIType entries : 69
```

```
INDEX : 1
```

```
-----
```

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

```
...
```

```
INDEX : 2
```

```
-----
```

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

```

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

```

EVB VMs Information

The following command displays all active VMs:

```
show virt evb vdp vm
```

Command mode: All

```

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

```

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

UFP Information

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

Table 47. *UFP Information Options*

Command Syntax and Usage
<p>show ufp [port <port_no.>] [vport <1-8>] [network qos evb]</p> <p>Displays the UFP network and QoS settings applied on all ports or on specified physical and virtual ports.</p> <ul style="list-style-type: none">o network filters only UFP network settingso qos filters only QoS network settingso evb filters only EVB profile settings <p>Command mode: All</p>
<p>show ufp information {cdcp qos tlvstat} [port <port_no.>]</p> <p>Displays global or port-specific UFP information on:</p> <ul style="list-style-type: none">o cdcp displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see page 104.o qos displays bandwidth allocation between virtual ports. For details, see page 104.o tlvstat displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see page 105. <p>Command mode: All</p>
<p>show ufp information getvlan <2-4094></p> <p>Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID.</p> <p>Command mode: All</p>
<p>show ufp information port [<port_no.>]</p> <p>Displays UFP status for all physical ports or only for a specified physical port. Information includes whether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see page 103.</p> <p>Command mode: All</p>
<p>show ufp information qos [port <port_no.>] [vport <1-8>]</p> <p>Displays bandwidth allocation between virtual ports for all physical ports or specified physical and virtual ports. For details, see page 104.</p> <p>Command mode: All</p>

Table 47. UFP Information Options

Command Syntax and Usage
<p>show ufp information vport [port <port_no.>] [vport <1-8>]</p> <p>Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see page 106.</p> <p>Command mode: All</p>
<p>show ufp information vlan [<1-4094>]</p> <p>Displays ports and vports associated to all configured VLANs or to a specified VLAN ID. For details, see page 107.</p> <p>Command mode: All</p>

Port Information

The following command displays UFP port information:

show ufp information port

Command mode: All

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

Port information includes the following for each physical port:

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

CDCP Information

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

show ufp information cdcp

Command mode: All

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

CDCP information includes the following for each physical port:

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

QoS Information

The following command displays Quality of Service information:

show ufp information qos

Command mode: All

```
Global UFP QoS mode: UFP QoS BW

Port | Vport | Mode | Minbw% | Maxbw% | Prio | HstCtrl
-----|-----|-----|-----|-----|-----|-----
INTA6 | 3     | ETS  |         |         | 3    | Dis
      | 4     | ETS  |         |         | 0    | Dis
-----|-----|-----|-----|-----|-----|-----
INTA8 | 1     | BW   | 30     | 100    |      | 
      | 2     | BW   | 30     | 100    |      | 
      | 3     | BW   | 10     | 100    |      | 
      | 4     | BW   | 10     | 100    |      | 
-----|-----|-----|-----|-----|-----|-----
INTA10| 1     | ETS  |         |         | 0    | Dis
      | 2     | ETS  |         |         | 3    | Dis
      | 3     | ETS  |         |         | 2    | Dis
      | 4     | ETS  |         |         | 0    | Dis
      | 5     | ETS  |         |         | 4    | Dis
      | 6     | ETS  |         |         | 5    | Dis
      | 7     | ETS  |         |         | 6    | Dis
      | 8     | ETS  |         |         | 7    | Dis
...  
```


QoS information includes the following:

- Physical port number
- Virtual port number
- Minimum guaranteed bandwidth allocated
- Maximum bandwidth achievable
- ETS or Bandwidth mode
- 802.1p priority associated to the vport
- Host control

TLV Status Information

The following command displays Type-Length-Values information:

```
show ufp information tlvstat
```

Command mode: All

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

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

Virtual Port Information

The following command displays virtual port information:

```
show ufp information vport
```

Command mode: All

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

Virtual port information includes the following for each virtual port:

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

VLAN Information

The following command displays VLAN information:

show ufp information vlan

Command mode: All

```
VLAN
----
 100

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

EXT Port list:
  EXT3     EXT4     EXT8     EXT9

INT Port list:
  INTB13

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

VMR Port list:
```

VLAN information includes the following for each VLAN:

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

TLV Information

The following commands display TLV information:

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

Command mode: All

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

UFP Capability Discovery TLV information includes the following:

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

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

Command mode: All

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

UFP Channel Discovery and Configuration Protocol TLV includes the following:

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

show ufp transmit linkdown port <port alias or number>

Command mode: All

```
UFP LINK-DOWN TLV transmitted on port INTA8:
Header  : Type 2 Length 3 Flags 0x0 Status 0x0
SCID   : 5
```

show ufp receive linkup port <port alias or number>

Command mode: All

```
UFP LINK-UP TLV received on port INTA9:
Header  : Type 3 Length 4 Flags 0x1 Status 0x0
SCID   : 6 9
```

show ufp receive prop port <port alias or number>

Command mode: All

```
UFP NIC-PROPS TLV transmitted on port INTA9:
Header  : Type 1 Length 17 Flags 0x0 Status 0x0
Props   : Channel Type 1 SCHED Type 0 Res 0x0 Num VLAN 0
SCID 6 SVID 4006 iSCSI 0 Host Pri 0 FCoE 0 TC 7 Min BW 0 Max BW
0
SCID 9 SVID 4009 iSCSI 0 Host Pri 0 FCoE 0 TC 2 Min BW 0 Max BW
0
```

DCBX Information Commands

The following commands display DCBX information.

Table 48. *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 49 describes the Converged Enhanced Ethernet (CEE) information options.

Table 49. *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 50](#) describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 50. *DCBX Information Options*

Command Syntax and Usage
show cee information dcbx port <i><port alias or number></i> Displays all DCBX information. Command mode: All
show cee information dcbx port <i><port alias or number></i> app_proto Displays information about the DCBX Application Protocol state machine on the selected port. For details, see page 117 . Command mode: All
show cee information dcbx port <i><port alias or number></i> control Displays information about the DCBX Control state machine for the selected port. For details, see page 113 . Command mode: All
show cee information dcbx port <i><port alias or number></i> ets Displays information about the DCBX ETS state machine. For details, see page 115 . Command mode: All
show cee information dcbx port <i><port alias or number></i> feature Displays information about the DCBX Feature state machine for the selected port. For details, see page 114 . Command mode: All
show cee information dcbx port <i><port alias or number></i> pfc Displays information about the DCBX PFC state machine. For details, see page 116 . Command mode: All

DCBX Control Information

The following command displays DCBX control information:

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

Command mode: All

DCBX Port Control State-machine Info						
=====						
Alias	Port	OperStatus	OperVer	MaxVer	SeqNo	AckNo

INTA1	1	enabled	0	0	0	0
INTA2	2	enabled	0	0	4	2
INTA3	3	enabled	0	0	0	0
INTA4	4	enabled	0	0	1	1
...						

DCBX control information includes the following:

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

DCBX Feature Information

The following command displays DCBX feature information:

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

Command mode: All

```

DCBX Port Feature State-machine Info
=====
Alias  Port  Type   AdmState Will  Advrt OpVer  MxVer PrWill SeqNo Err OperMode Syncd
-----
INTA2  2     ETS    enabled No   Yes   0     0     Yes   1    No  enabled  Yes
INTA2  2     PFC    enabled No   Yes   0     0     Yes   1    No  enabled  Yes
INTA2  2     AppProt disabled No   Yes   0     0     Yes   1    No  disabled Yes
...

```

The following table describes the DCBX feature information.

Table 51. DCBX Feature Information Fields

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

DCBX ETS Information

The following command displays DCBX ETS information:

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

Command mode: All

DCBX Port Priority Group - Priority Allocation Table					
Alias	Port	Priority	PgIdDes	PgIdOper	PgIdPeer
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 52. 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 53. DCBX Application Protocol Information Fields

Parameter	Description
Protocol ID	Identifies the supported Application Protocol.
Selector Field	Specifies the Application Protocol type, as follows: <ul style="list-style-type: none"> o 0 = Ethernet Type o 1 = TCP socket ID
Organizationally Unique ID	DCBX TLV identifier

Table 53. *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 54 describes the Enhanced Transmission Selection (ETS) information options.

Table 54. *ETS Information Options*

Command Syntax and Usage
<p>show cee global ets [information] Displays global ETS information. Command mode: All</p>
<p>show cee global ets priority-group <0-7, 15> Displays the current global ETS Priority Group parameters. Command mode: All</p>

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 55 describes the Priority Flow Control (PFC) information options.

Table 55. *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 56 describes the Fibre Channel over Ethernet (FCoE) information options.

Table 56. *FCoE Information Options*

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

FIP Snooping Information

Table 57 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options.

Table 57. *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 58. *Statistics Commands*

Command Syntax and Usage
<p>show counters</p> <p>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 191.</p> <p>Command mode: All</p>
<p>show layer3 counters</p> <p>Displays Layer 3 statistics.</p> <p>Command mode: All</p>
<p>show ntp counters</p> <p>Displays Network Time Protocol (NTP) Statistics. See page 188 for a sample output and a description of NTP Statistics.</p> <p>Command mode: All</p>
<p>show snmp-server counters</p> <p>Displays SNMP statistics. See page 184 for sample output.</p> <p>Command mode: All</p>

Forwarding Database Statistics

The following commands display Forwarding Database statistics.

Table 59. *Forwarding Database statistics commands*

Command Syntax and Usage
<p>show mac-address-table counters [all]</p> <p>Displays Forwarding Database (FDB) statistics. The all options displays all FDB statistics (unicast and multicast).</p> <p>Command mode: All</p>
<p>show mac-address-table counters interface port <i><port alias or number></i></p> <p>Displays Forwarding Database (FDB) statistics for the specified port.</p> <p>Command mode: All</p>
<p>show mac-address-table counters portchannel <i><trunk group number></i></p> <p>Displays Forwarding Database (FDB) statistics for the specified trunk group.</p> <p>Command mode: All</p>
<p>show mac-address-table counters state {forward trunk unknown}</p> <p>Displays Forwarding Database (FDB) statistics by state:</p> <ul style="list-style-type: none">o forward displays FDB statistics for forwarding state MAC address entrieso trunk displays FDB statistics for trunk state MAC address entrieso unknown displays FDB statistics for unknown state MAC address entries <p>Command mode: All</p>
<p>show mac-address-table counters static</p> <p>Displays Forwarding Database (FDB) statistics for static MAC address entries.</p> <p>Command mode: All</p>
<p>show mac-address-table counters unicast</p> <p>Displays Forwarding Database (FDB) statistics for unicast MAC address entries.</p> <p>Command mode: All</p>
<p>show mac-address-table counters vlan <i><VLAN number></i></p> <p>Displays Forwarding Database (FDB) statistics for the specified VLAN.</p> <p>Command mode: All</p>
<p>clear mac-address-table counters</p> <p>Clears Forwarding Database (FDB) statistics.</p> <p>Command mode: All except User EXEC</p>

Port Statistics

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

Table 60. *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 129 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 130 for sample output. Command mode: All
show interface port <port alias or number> interface-counters Displays interface statistics for the specified port. See page 133 for sample output. Command mode: All
show interface port <port alias or number> ip-counters Displays IP statistics for the specified port. See page 136 for sample output. Command mode: All
show interface port <port alias or number> link-counters Displays link statistics for the specified port. See page 136 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 60. *Port Statistics Commands*

Command Syntax and Usage
<p>show interface port <i><port alias or number></i> oam counters</p> <p>Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.</p> <p>Command mode: All</p>
<p>show interface port <i><port alias or number></i> rmon-counters</p> <p>Displays Remote Monitoring (RMON) statistics for the port. See page 137 for sample output.</p> <p>Command mode: All</p>
<p>clear counters</p> <p>Clears statistics for all ports.</p> <p>Command mode: All except User EXEC</p>
<p>clear interface port <i><port alias or number></i> counters</p> <p>Clears all statistics for the port.</p> <p>Command mode: All except User EXEC</p>

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 61. *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 62. Ethernet Statistics for Port

Statistics	Description
dot3StatsAlignmentErrors	<p>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.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> 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.</p>
dot3StatsFCSErrors	<p>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.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> 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.</p>

Table 62. Ethernet Statistics for Port (continued)

Statistics	Description
dot3StatsSingleCollision Frames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p>
dot3StatsMultipleCollision Frames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p>
dot3StatsLateCollisions	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>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.</p>
dot3StatsExcessive Collisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMac TransmitErrors	<p>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 <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>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.</p>

Table 62. *Ethernet Statistics for Port (continued)*

Statistics	Description
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> 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.</p>
dot3StatsInternalMacReceiveErrors	<p>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 <code>dot3StatsFrameTooLongs</code> object, the <code>dot3StatsAlignmentErrors</code> object, or the <code>dot3StatsFCSErrors</code> object.</p> <p>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.</p>

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 63. *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 63. *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 <code>ifOutBroadcastPkts</code> .
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 <code>ifOutMulticastPkts</code> .
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 63. *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 64. *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 65. *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 66. 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 66. *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 66. *RMON Statistics of a Port (continued)*

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

QoS Queue Statistics

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

Table 67. *QoS Queue Statistics*

Command Syntax and Usage
<p>show interface port <i><port alias or number></i> egress-queue-counters [<i><0-7></i> drop]</p> <p>Displays the total number of successfully transmitted or dropped packets and bytes for each QoS queue for the selected port.</p> <ul style="list-style-type: none">o <i><0-7></i> displays statistics only for the specified queueo drop displays statistics only for the dropped packets and bytes <p>Command mode: All</p>
<p>show interface port <i><port alias or number></i> egress-mcast-queue-counters [<i><8-11></i> drop]</p> <p>Displays the total number of successfully transmitted or dropped packets and bytes for each multicast QoS queue for the selected port.</p> <ul style="list-style-type: none">o <i><8-11></i> displays statistics only for the specified queueo drop displays statistics only for the dropped packets and bytes <p>Command mode: All</p>
<p>show interface port <i><port alias or number></i> egress-queue-rate [<i><0-7></i> drop]</p> <p>Displays the number of successfully transmitted or dropped packets and bytes per second for each QoS queue for the selected port.</p> <ul style="list-style-type: none">o <i><0-7></i> displays statistics only for the specified queueo drop displays statistics only for the dropped packets and bytes <p>Command mode: All</p>
<p>show interface port <i><port alias or number></i> egress-mcast-queue-rate [<i><8-11></i> drop]</p> <p>Displays the number of successfully transmitted or dropped packets and bytes per second for each multicast QoS queue for the selected port.</p> <ul style="list-style-type: none">o <i><8-11></i> displays statistics only for the specified queueo drop displays statistics only for the dropped packets and bytes <p>Command mode: All</p>

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

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

Command mode: All

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

Table 68. QoS Queue Rate-Based Statistics of a Port

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

Table 68. QoS Queue Rate-Based Statistics of a Port (continued)

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

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

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

Command mode: All

```

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

```

Table 69. *QoS Queue Rate-Based Statistics of a Port*

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

Link Aggregation Group (LAG) Statistics

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

Table 70. LAG Statistics Commands

Command Syntax and Usage
<pre>show interface portchannel <trunk group number> interface-counters</pre> <p>Displays interface statistics for the LAG. For a sample output see page 144.</p> <p>Command mode: All</p>
<pre>clear interface portchannel <trunk group number> counters</pre> <p>Clears all the statistics on the specified LAG.</p> <p>Command mode: All except User EXEC</p>

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 71. *Layer 2 Statistics Commands*

Command Syntax and Usage
show fcoe counters Displays Fibre Channel over Ethernet (FCoE) statistics. See page 183 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 146 for sample output. Command mode: All
show interface port <port alias or number> lldp counters Displays LLDP statistics for the specified port. See page 148 for sample output. Command mode: All except User EXEC
show hotlinks counters Displays Hot Links statistics. See page 147 for sample output. Command mode: All except User EXEC
show oam counters Displays OAM statistics. See page 149 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 LACPDU received:          - 870
Valid Marker PDU received:     - 0
Valid Marker Rsp PDU received: - 0
Unknown version/TLV type:      - 0
Illegal subtype received:      - 0
LACPDU transmitted:           - 6031
Marker PDU transmitted:        - 0
Marker Rsp PDU transmitted:    - 0
```

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

Table 72. *LACP Statistics*

Statistic	Description
Valid LACPDU received	Total number of valid LACP data units received.
Valid Marker PDU received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDU 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.
LACPDU transmitted	Total number of LACP data units transmitted.
Marker PDU transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDU 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 73. *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 74. *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 Rx :      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 75. *Layer 3 Statistics Commands*

Command Syntax and Usage
show ip counters Displays IP statistics. See page 152 for sample output. Command mode: All
show ip dns counters Displays Domain Name System (DNS) statistics. See page 161 for sample output. Command mode: All
show ip 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 164 for sample output. Command mode: All
show ip igmp vlan <VLAN number> counter Displays IGMP statistics for a specific VLAN. See page 164 for sample output. Command mode: All
show ip slp counter Displays Service Location Protocol (SLP) packet statistics. See page 190 for a sample output. Command mode: All
show ip tcp counters Displays TCP statistics. See page 161 for sample output. Command mode: All
show ip udp counters Displays UDP statistics. See page 163 for sample output. Command mode: All
show ipv6 counters Displays IPv6 statistics. See page 155 for sample output. Command mode: All

Table 75. *Layer 3 Statistics Commands (continued)*

Command Syntax and Usage
<p>clear ip counters</p> <p>Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics.</p> <p>Command mode: All except User EXEC</p>
<p>clear ip dns counters</p> <p>Clears Domain Name System (DNS) statistics.</p> <p>Command mode: All except User EXEC</p>
<p>clear ip igmp [<VLAN number>] counters</p> <p>Clears IGMP statistics for all VLANs or for a specific VLAN.</p> <p>Command mode: All</p>
<p>clear ip slp counters</p> <p>Clears Service Location Protocol (SLP) packet statistics.</p> <p>Command mode: All except user EXEC</p>
<p>clear ip tcp counters</p> <p>Clears Transmission Control Protocol (TCP) statistics.</p> <p>Command mode: All except User EXEC</p>
<p>clear ip udp counters</p> <p>Clears User Datagram Protocol (UDP) statistics.</p> <p>Command mode: All except User EXEC</p>
<p>clear ipv6 counters</p> <p>Clears IPv6 statistics. Use this command with caution as it deletes all the IPv6 statistics.</p> <p>Command mode: All except User EXEC</p>
<p>show layer3 counters</p> <p>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.</p> <p>Command mode: All</p>

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 76. *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 76. *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 <i>no-route</i> 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 76. *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 ICMEchoReq        0 ICMEchoReps
  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 PktTooBigMsg            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 77 describes the IPv6 statistics.

Table 77. *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 77. 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 78. *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 78. *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 79 describes the UDP statistics.

Table 79. *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

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 80. 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 81. *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 82. *TCP Statistics*

Statistic	Description
tcpRtoAlgorithm	The algorithm used to determine the <code>timeout</code> value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>LBOUND</code> quantity described in RFC 793.

Table 82. *TCP Statistics (continued)*

Statistic	Description
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission <code>timeout</code> , measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission <code>timeout</code> . In particular, when the <code>timeout</code> algorithm is <code>rsre(3)</code> , an object of this type has the semantics of the <code>UBOUND</code> 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 <code>SYN-SENT</code> state from the <code>CLOSED</code> state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the <code>SYN-RCVD</code> state from the <code>LISTEN</code> state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>SYN-SENT</code> state or the <code>SYN-RCVD</code> state, plus the number of times TCP connections have made a direct transition to the <code>LISTEN</code> state from the <code>SYN-RCVD</code> state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the <code>CLOSED</code> state from either the <code>ESTABLISHED</code> state or the <code>CLOSE-WAIT</code> 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 <code>ESTABLISHED</code> state.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the <code>RST</code> 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 83. *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 84. 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 84. *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 85. *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 167 . 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 177 . 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 178 . 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 178 . Command mode: All
show processes cpu history Displays history of CPU utilization. To view a sample output, see page 180 . Command mode: All

Packet Statistics

The following commands display Packet statistics.

Table 86. *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 167 . Command mode: All
clear mp packet logs Clears all CPU packet statistics and logs. Command mode: Privileged EXEC

MP Packet Statistics

The following command displays MP packet statistics:

show mp packet counters

Command mode: All

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

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

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

```

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

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

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

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

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

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

```

Table 87. *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 87. *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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 87. *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 87. *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 88. *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 172 . 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 89. *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 172 . 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 90. *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 91](#).

Table 91. Packet Log Parsing Options

Command Syntax and Usage
<pre>show mp packet parse {rx tx} bpdud</pre> <p>Displays only BPDUs logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} cisco</pre> <p>Displays only Cisco packets (BPDU/CDP/UDLD) logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} fcoe</pre> <p>Displays only FCoE FIP PDUs logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} ftp</pre> <p>Displays only FTP packets logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} http</pre> <p>Displays only HTTP packets logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} https</pre> <p>Displays only HTTPS packets logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} igmp</pre> <p>Displays only IGMP packets logged. Command mode: All</p>
<pre>show mp packet parse {rx tx} ip-addr <IPv4_address></pre> <p>Displays only logged packets with the specified IPv4 address. Command mode: All</p>
<pre>show mp packet parse {rx tx} ipv4</pre> <p>Displays only IPv4 packets logged. Command mode: All</p>

Table 91. *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 91. *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
147e6808:  0.0.0.0                0 <=>
           0.0.0.0                23 listen
147e66b8:  0:0:0:0:0:0:0:0             0 <=>
           0:0:0:0:0:0:0:0             23 listen
147e6568:  0.0.0.0                0 <=>
           0.0.0.0                23 listen

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

```

Table 92. *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 93. 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
  ID    Name         1sec      5sec      1Min      5Min      Status
-----
  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 94. 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 94. *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 95. *ACL Statistics Commands*

Command Syntax and Usage
show access-control counters Displays all ACL statistics. For output sample, see page 182 . Command mode: All
show access-control list <1-256> counters Displays the Access Control List Statistics for a specific ACL. Command mode: All
show access-control list6 <1-128> counters Displays the IPv6 ACL statistics for a specific ACL. Command mode: All
show access-control meter <1-127> counters Displays ACL meter statistics. For output sample, see page 182 . Command mode: All
show access-control vmap <1-128> counters Displays VLAN Map statistics for the selected VMAP. For details, see page 182 . Command mode: All
clear access-control list {<1-256> all} counters Clears ACL statistics. Command mode: Privileged EXEC
clear access-control list6 {<1-128> all} Clears IPv6 ACL statistics. Command mode: Privileged EXEC
clear access-control meter <1-127> counters Clears ACL meter statistics. Command mode: Privileged EXEC

ACL Statistics

The following command displays ACL statistics.

show access-control counters

Command mode: All

Hits for ACL 1:	26057515
Hits for ACL 2:	26057497

ACL Meter Statistics

This option displays ACL meter statistics.

show access-control meter <meter number> counters

Command mode: All

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

VMAP Statistics

The following command displays VLAN Map statistics.

show access-control vmap <vmap number> counters

Command mode: All

Hits for VMAP 1:	57515
------------------	-------

Fibre Channel over Ethernet Statistics

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

show fcoe counters

Command mode: All

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

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

Table 96. *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
snmpInTooBig:	0	snmpInNoSuchNames:	0
snmpInBadValues:	0	snmpInReadOnlys:	0
snmpInGenErrs:	0	snmpInTotalReqVars:	798464
snmpInTotalSetVars:	2731	snmpInGetRequests:	17593
snmpInGetNexts:	131389	snmpInSetRequests:	615
snmpInGetResponses:	0	snmpInTraps:	0
snmpOutTooBig:	0	snmpOutNoSuchNames:	1
snmpOutBadValues:	0	snmpOutReadOnlys:	0
snmpOutGenErrs:	1	snmpOutGetRequests:	0
snmpOutGetNexts:	0	snmpOutSetRequests:	0
snmpOutGetResponses:	150093	snmpOutTraps:	4
snmpSilentDrops:	0	snmpProxyDrops:	0

Table 97. *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 97. *SNMP Statistics (continued)*

Statistic	Description
snmpInASNParseErrs	<p>The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received.</p> <p>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.</p>
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.
snmpInTooBig	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 <i>too big</i> .
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 <i>noSuchName</i> .
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 <i>badValue</i> .
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 <i>'read-Only'</i> . It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value <i>'read-Only'</i> in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.

Table 97. *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 <code>genErr</code> .
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.
snmpOutTooBig	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 <code>too big</code> .
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 <code>noSuchName</code> .
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 <code>badValue</code> .
snmpOutReadOnly	Not in use.

Table 97. *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 <code>genErr</code> .
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 <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -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 <code>GetRequest</code> -PDUs, <code>GetNextRequest</code> -PDUs, <code>GetBulkRequest</code> -PDUs, <code>SetRequest</code> -PDUs, and <code>InformRequest</code> -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 98. *NTP Statistics*

Field	Description
Primary Server	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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 98. *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.

SLP Statistics

The following table displays SLP statistics commands:

Table 99. *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 100. *General Configuration Commands*

Command Syntax and Usage
<p>show running-config [diff]</p> <p>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 352.</p> <p>Command mode: All except User EXEC</p>
<p>copy running-config backup-config</p> <p>Copy the current (running) configuration from switch memory to the backup-config partition. For details, see page 353.</p> <p>Command mode: All except User EXEC</p>
<p>copy running-config startup-config</p> <p>Copy the current (running) configuration from switch memory to the startup-config partition.</p> <p>Command mode: All except User EXEC</p>
<p>copy running-config {ftp sftp tftp} [extm-port mgt-port]</p> <p>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.</p> <p>Command mode: All except User EXEC</p>
<p>copy {ftp sftp tftp} running-config [extm-port mgt-port]</p> <p>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 354.</p> <p>Command mode: All except User EXEC</p>
<p>copy {sftp tftp} public-key [extm-port mgt-port]</p> <p>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:</p> <ul style="list-style-type: none">o public-key: client public keyo extm-port: external management porto mgt-port: management port <p>Command mode: All except User EXEC</p>

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 SI4093 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 4093# copy running-config startup-config
```

or

```
SI 4093# write
```

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

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see [“Selecting a Configuration Block” on page 375](#).

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 101. *System Configuration Commands*

Command Syntax and Usage
<p>[no] banner <1-80 characters></p> <p>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 <code>show sys-info</code> command.</p> <p>Command mode: Global configuration</p>
<p>[no] boot strict enable</p> <p>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.</p> <p>Setting will be applied and device will be reset to default factory configuration after reboot.</p> <p>The default setting is disabled.</p> <p>Note: Ensure NIST Strict compliance is enabled on the Chassis Management Module before enabling Strict mode operation on the device.</p> <p>Command mode: Global configuration</p>
<p>[no] hostname <character string></p> <p>Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).</p> <p>Command mode: Global configuration</p>
<p>line console length <0-300></p> <p>Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging.</p> <p>The default value is 28.</p> <p>Command mode: Global configuration</p>
<p>no line console</p> <p>Sets <code>line console length</code> to the default value of 28.</p> <p>Command mode: Global configuration</p>
<p>line vty length <0-300></p> <p>Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging.</p> <p>The default value is 28.</p> <p>Command mode: Global configuration</p>

Table 101. *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 101. System Configuration Commands (continued)

Command Syntax and Usage
<p>system internal-VLAN <VLAN range (2-4094)> [black-hole vlan <VLAN ID>]</p> <p>Configures a range of System Reserved VLANs. The black-hole option also configures the Black-hole VLAN.</p> <p>The default reserved VLAN is 4091. This is also the default Black-hole VLAN.</p> <p>Note: The Black-hole VLAN must be in the configured system reserved VLAN range for the command to be valid.</p> <p>Command mode: Global configuration</p>
<p>system linkscan {fast normal slow}</p> <p>Configures the link scan interval used to poll the status of ports.</p> <p>Command mode: Global configuration</p>
<p>[no] system notice <maximum 1024 character multi-line login notice> <'.' to end></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>[no] system packet-logging</p> <p>Enables or disables logging of packets that come to the CPU.</p> <p>The default setting is enabled.</p> <p>Command mode: Global configuration</p>
<p>[no] system reset-control</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>system time <hh>:<mm>:<ss></p> <p>Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.</p> <p>Command mode: Global configuration</p>
<p>system timezone</p> <p>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.</p> <p>Command mode: Global configuration</p>

Table 101. *System Configuration Commands (continued)*

Command Syntax and Usage
<p>terminal dont-ask</p> <p>Disables CLI confirmation prompts for the current session. The switch will choose the default answer.</p> <p>Note: When using this command any settings configured through the prompting command will be temporarily disregarded for the duration of the current session.</p> <p>Command mode: All</p>
<p>no terminal dont-ask</p> <p>Enables CLI confirmation prompts for the current session.</p> <p>Note: When using this command any settings configured through the prompting command will be temporarily disregarded for the duration of the current session.</p> <p>Command mode: All</p>
<p>terminal-length <0-300></p> <p>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 <code>line vty length</code> or <code>line console length</code> value in effect at login.</p> <p>Command mode: All</p>
<p>show boot strict</p> <p>Displays the current security strict mode status.</p> <p>Command mode: Global configuration</p>
<p>show system</p> <p>Displays the current system parameters.</p> <p>Command mode: All</p>

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 102. *Error Disable Configuration Commands*

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

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 103. *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 104. *Host Log Configuration Commands*

Command Syntax and Usage
<p>[no] logging buffer severity <0-7></p> <p>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.</p> <p>The default is 7, which means log all severity levels.</p> <p>Command mode: Global configuration</p>
<p>[no] logging console</p> <p>Enables or disables delivering syslog messages to the console. When necessary, disabling <code>console</code> ensures the switch is not affected by syslog messages.</p> <p>The default setting is <code>enabled</code>.</p> <p>Command mode: Global configuration</p>
<p>logging console severity <0-7></p> <p>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.</p> <p>The default is 7, which means log all severity levels.</p> <p>Command mode: Global configuration</p>
<p>no logging console severity</p> <p>Disables delivering syslog messages to the console based on severity.</p> <p>Command mode: Global configuration</p>
<p>logging host <1-2> address <IP address> [extm-port mgt-port]</p> <p>Sets the IPv4 address of the first or second syslog host.</p> <p>Command mode: Global configuration</p>
<p>logging host <1-2> address6 <IPv6 address> [extm-port mgt-port]</p> <p>Sets the IPv6 address of the first or second syslog host.</p> <p>Command mode: Global configuration</p>
<p>logging host <1-2> facility <0-7></p> <p>This option sets the facility level of the first or second syslog host displayed.</p> <p>The default is 0.</p> <p>Command mode: Global configuration</p>

Table 104. Host Log Configuration Commands

Command Syntax and Usage
<p>logging host <1-2> severity <0-7></p> <p>This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels.</p> <p>Command mode: Global configuration</p>
<p>no logging host <1-2></p> <p>Removes the specified syslog host.</p> <p>Command mode: Global configuration</p>
<p>[no] logging log {all <feature>}</p> <p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlangs, stg, or ssh), or enable/disable syslog on all available features.</p> <p>Command mode: Global configuration</p>
<p>[no] logging pdrop enable</p> <p>Enables or disables packet drop logging.</p> <p>By default, the switch generates these messages once every 30 minutes.</p> <p>Command mode: Global configuration</p>
<p>logging pdrop interval <0-30></p> <p>Sets the packet drop logging interval, in minutes.</p> <p>The default value is 30.</p> <p>Command mode: Global configuration</p>
<p>[no] logging synchronous [level <0-7> all]</p> <p>Enables or disables synchronous logging messages. When enabled, logging messages are displayed asynchronously.</p> <p>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.</p> <p>The default setting is 2.</p> <p>Command mode: Global configuration</p>
<p>logging source-interface loopback <1-5></p> <p>Sets the loopback interface number for syslogs.</p> <p>Command mode: Global configuration</p>

Table 104. *Host Log Configuration Commands*

Command Syntax and Usage
<p>no logging source-interface loopback</p> <p>Removes the loopback interface for syslogs.</p> <p>Command mode: Global configuration</p>
<p>show logging [severity <severity level>] [reverse]</p> <p>Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see page 40.</p> <p>The reverse option displays the output in reverse order, from the newest entry to the oldest.</p> <p>Command mode: All</p>

SSH Server Configuration

For the SI4093 System Interconnect Module, these commands enable Secure Shell access from any SSH client.

Table 105. *SSH Server Configuration Commands*

Command Syntax and Usage
<p>[no] ssh enable Enables or disables the SSH server. Command mode: Global configuration</p>
<p>ssh generate-host-key Generate the RSA host key. Command mode: Global configuration</p>
<p>ssh maxauthattempts <1-20> Sets the maximum number of SSH authentication attempts. The default value is 2. Command mode: Global configuration</p>
<p>no ssh maxauthattempts Resets the maximum number of SSH authentication attempts to its default value of 2. Command mode: Global configuration</p>
<p>ssh port <TCP port number> Sets the SSH server port number. The default port number is 22. Command mode: Global configuration</p>
<p>no ssh port Resets the SSH server port to the default port number 22. Command mode: Global configuration</p>
<p>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</p>
<p>[no] ssh scp-enable Enables or disables the SCP apply and save. Command mode: Global configuration</p>
<p>ssh scp-password Set the administration password for SCP access. Command mode: Global configuration</p>

Table 105. *SSH Server Configuration Commands*

Command Syntax and Usage
<p>show ssh</p> <p>Displays the current SSH server configuration.</p> <p>Command mode: All</p>
<p>show ssh-clienthostkey {address <SFTP server IP address> all}</p> <p>Displays the current SFTP/SSH host key configuration.</p> <ul style="list-style-type: none">o address: Displays a specific SFTP/SSH host keyo all: Displays all SFTP/SSH host keys <p>Commands mode: All</p>
<p>show ssh-clientpubkey {all index <1-100> username <user name>}</p> <p>Displays the current SSH public key configuration.</p> <ul style="list-style-type: none">o all: Displays all SSH public keyso index: Displays a specific SSH public keyo username: Displays all the SSH public keys of a particular user <p>Command mode: All</p>
<p>clear ssh-clienthostkey {address <SFTP server IP address> all}</p> <p>Clears stored SFTP/SSH host key configuration.</p> <ul style="list-style-type: none">o address: Clears a specific SFTP/SSH host keyo all: Clears all SFTP/SSH host keys <p>Command mode: All except User EXEC</p>
<p>clear ssh-clientpubkey {all index <1-100> username <user name>}</p> <p>Clears stored SSH public key configuration.</p> <ul style="list-style-type: none">o all: Clears all SSH public keyso index: Clears a specific SSH public keyo username: Clears a particular username from all the SSH public keys <p>Command mode: All except User EXEC</p>

RADIUS Server Configuration

The following table displays RADIUS Server configuration commands.

Table 106. RADIUS Server Configuration Commands

Command Syntax and Usage
<p>[no] radius-server backdoor</p> <p>Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is <code>disabled</code>.</p> <p>To obtain the RADIUS backdoor password for your switch, contact your Service and Support line.</p> <p>Command mode: Global configuration</p>
<p>[no] radius-server enable</p> <p>Enables or disables the RADIUS server.</p> <p>Command mode: Global configuration</p>
<p>[default] radius-server port <UDP port number></p> <p>Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.</p> <p>Command mode: Global configuration</p>
<p>[no] radius-server primary-host <IP address></p> <p>Sets the primary RADIUS server address.</p> <p>Command mode: Global configuration</p>
<p>[no] radius-server secondary-host <IP address></p> <p>Sets the secondary RADIUS server address.</p> <p>Command mode: Global configuration</p>
<p>radius-server primary-host <hostname or IP address> [key <1-32 characters>]</p> <p>This is the primary shared secret between the switch and the RADIUS server(s). The <code>key</code> option sets the RADIUS server secret key.</p> <p>Command mode: Global configuration</p>
<p>no radius-server primary-host [key]</p> <p>Removes the primary RADIUS server. The <code>key</code> option removes only the RADIUS server secret key.</p> <p>Command mode: Global configuration</p>
<p>radius-server retransmit <1-3></p> <p>Sets the number of failed authentication requests before switching to a different RADIUS server.</p> <p>The default is 3 requests.</p> <p>Command mode: Global configuration</p>

Table 106. RADIUS Server Configuration Commands

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

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 107. TACACS+ Server Configuration Commands

Command Syntax and Usage
<p>[no] tacacs-server accounting-enable Enables or disables TACACS+ accounting. Command mode: Global configuration</p>
<p>[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</p>
<p>[no] tacacs-server backdoor Enables or disables the TACACS+ back door for Telnet, SSH/SCP or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default setting is disabled. To obtain the TACACS+ backdoor password for your SI4093, contact your Service and Support line. Command mode: Global configuration</p>
<p>tacacs-server chpassp <1-32 characters> Defines the password for the primary TACACS+ server. Command mode: Global configuration</p>

Table 107. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p>tacacs-server chpasswd <1-32 characters></p> <p>Defines the password for the secondary TACACS+ server.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server command-authorization</p> <p>Enables or disables TACACS+ command authorization.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server command-logging</p> <p>Enables or disables TACACS+ command logging.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server directed-request [restricted no-truncate]</p> <p>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.</p> <p>This command allows the following options:</p> <ul style="list-style-type: none">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. <p>Command mode: Global configuration</p>
<p>[no] tacacs-server enable</p> <p>Enables or disables the TACACS+ server.</p> <p>By default, the server is disabled.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server enable-bypass</p> <p>Enables or disables the enable-bypass for administrator privilege.</p> <p>By default, enable-bypass is enabled.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server encryption-enable</p> <p>Enables or disables encryption for TACACS+ traffic packets.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server password-change</p> <p>Enables or disables TACACS+ password change.</p> <p>The default value is disabled.</p> <p>Command mode: Global configuration</p>

Table 107. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p>primary-password</p> <p>Configures the password for the primary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p>
<p>secondary-password</p> <p>Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p>
<p>[default] tacacs-server port <TCP port number></p> <p>Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server primary-host <IP address></p> <p>Defines the primary TACACS+ server address.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server primary-host <IP address> key <1-32 characters></p> <p>This is the primary shared secret key between the switch and the TACACS+ server(s).</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server privilege-mapping</p> <p>Enables or disables TACACS+ privilege-level mapping. The default value is disabled.</p> <p>Command mode: Global configuration</p>
<p>tacacs-server retransmit <1-3></p> <p>Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server secondary-host <IP address></p> <p>Defines the secondary TACACS+ server address.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server secondary-host <IP address> key <1-32 characters></p> <p>This is the secondary shared secret key between the switch and the TACACS+ server(s).</p> <p>Command mode: Global configuration</p>

Table 107. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
<p>[no] tacacs-server secure-backdoor</p> <p>Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.</p> <p>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.</p> <p>The default is <code>disabled</code>.</p> <p>Command mode: Global configuration</p>
<p>tacacs-server timeout <4-15></p> <p>Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed.</p> <p>The default is 5 seconds.</p> <p>Command mode: Global configuration</p>
<p>[no] tacacs-server user-mapping {<0-15> user oper admin}</p> <p>Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.</p> <p>Command mode: Global configuration</p>
<p>show tacacs-server</p> <p>Displays current TACACS+ configuration parameters.</p> <p>Command mode: All</p>

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 108. LDAP Server Configuration Commands

Command Syntax and Usage
<p>ldap-server attribute username <1-128 characters></p> <p>Sets a customized LDAP user attribute.</p> <p>The default value is <code>uid</code>.</p> <p>Note: The user attribute needs to be set to <code>cn</code> if LDAP server is MS active directory.</p> <p>Command mode: Global configuration</p>
<p>no ldap-server attribute [username]</p> <p>Sets LDAP attributes back to their default values. The <code>username</code> option sets the LDAP user attribute back to its default value of <code>uid</code>.</p> <p>Command mode: Global configuration</p>
<p>[no] ldap-server backdoor</p> <p>Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS.</p> <p>The default setting is <code>disabled</code>.</p> <p>Note: To obtain the LDAP back door password for your SI4093, contact your Service and Support line.</p> <p>Command mode: Global configuration</p>
<p>ldap-server domain [<1-128 characters> none]</p> <p>Sets the domain name for the LDAP server. Enter the full path for your organization. For example:</p> <p><code>ou=people,dc=mydomain,dc=com</code></p> <p>Command mode: Global configuration</p>
<p>[no] ldap-server enable</p> <p>Enables or disables the LDAP server.</p> <p>Command mode: Global configuration</p>
<p>[default] ldap-server port <UDP port number></p> <p>Enter the number of the UDP port to be configured, between 1 - 65000.</p> <p>The default is 389.</p> <p>Command mode: Global configuration</p>
<p>[no] ldap-server primary-host <IP address></p> <p>Sets the primary LDAP server address.</p> <p>Command mode: Global configuration</p>

Table 108. *LDAP Server Configuration Commands (continued)*

Command Syntax and Usage
<p>ldap-server retransmit <1-3></p> <p>Sets the number of failed authentication requests before switching to a different LDAP server.</p> <p>The default is 3 requests.</p> <p>Command mode: Global configuration</p>
<p>[no] ldap-server secondary-host <IP address></p> <p>Sets the secondary LDAP server address.</p> <p>Command mode: Global configuration</p>
<p>ldap-server timeout <4-15></p> <p>Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed.</p> <p>The default is 5 seconds.</p> <p>Command mode: Global configuration</p>
<p>show ldap-server</p> <p>Displays the current LDAP server parameters.</p> <p>Command mode: All</p>

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 109. *NTP Server Configuration Commands*

Command Syntax and Usage
<p>[no] ntp authenticate</p> <p>Enables or disables NTP authentication. When authentication is enabled, the switch transmits NTP packets with the MAC address appended.</p> <p>The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<p>[no] ntp enable</p> <p>Enables or disables the NTP synchronization service.</p> <p>Command mode: Global configuration</p>
<p>ntp interval <5-44640></p> <p>Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server.</p> <p>The default value is 1440.</p> <p>Command mode: Global configuration</p>
<p>ntp primary-key <1-65534></p> <p>Adds the NTP primary server key, which specifies which MD5 key is used by the primary server.</p> <p>Command mode: Global configuration</p>
<p>ntp secondary-key <1-65534></p> <p>Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server.</p> <p>Command mode: Global configuration</p>
<p>ntp primary-server <IP address> [extm-port mgt-port]</p> <p>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:</p> <ul style="list-style-type: none"> o external management port (extm) o internal management port (mgt) <p>Command mode: Global configuration</p>
<p>no ntp primary-server</p> <p>Removes the primary NTP server address.</p> <p>Command mode: Global configuration</p>

Table 109. NTP Server Configuration Commands

Command Syntax and Usage
<p>ntp secondary-server <IP address> [extm-port mgt-port]</p> <p>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:</p> <ul style="list-style-type: none"> o external management port (extm) o internal management port (mgt) <p>Command mode: Global configuration</p>
<p>no ntp secondary-server</p> <p>Removes the secondary NTP server address.</p> <p>Command mode: Global configuration</p>
<p>ntp ipv6 primary-server <IPv6 address> [extm-port mgt-port]</p> <p>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:</p> <ul style="list-style-type: none"> o external management port (extm) o internal management port (mgt) <p>Command mode: Global configuration</p>
<p>no ntp ipv6 primary-server</p> <p>Removes the IPv6 primary NTP server address.</p> <p>Command mode: Global configuration</p>
<p>ntp ipv6 secondary-server <IPv6 address> [extm-port mgt-port]</p> <p>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:</p> <ul style="list-style-type: none"> o external management port (extm) o internal management port (mgt) <p>Command mode: Global configuration</p>
<p>no ntp ipv6 secondary-server</p> <p>Removes the IPv6 secondary NTP server address.</p> <p>Command mode: Global configuration</p>
<p>[no] ntp trusted-key <1-65534></p> <p>Adds or removes an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code.</p> <p>Command mode: Global configuration</p>
<p>show ntp</p> <p>Displays the current NTP service settings.</p> <p>Command mode: All</p>

NTP MD5 Key Commands

The following table displays NTP MD5 Key configuration commands.

Table 110. *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 111. *System SNMP Commands*

Command Syntax and Usage
<p>[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</p>
<p>[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</p>
<p>snmp-server host <trap host IP address> <trap host community string> Adds a trap host server. Command mode: Global configuration</p>
<p>no snmp-server host <trap host IP address> Removes the trap host server. Command mode: Global configuration</p>

Table 111. *System SNMP Commands*

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

Table 111. *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 112. *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 223 . 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 225 . 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 224 . Command mode: Global configuration

Table 112. *SNMPv3 Configuration Commands (continued)*

<p>snmp-server notify <1-16></p> <p>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 228.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-address <1-16></p> <p>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 226.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-parameters <1-16></p> <p>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 227.</p> <p>Command mode: Global configuration</p>
<p>snmp-server user <1-17></p> <p>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 221.</p> <p>Command mode: Global configuration</p>
<p>snmp-server version {v1v2v3 v3only}</p> <p>This command allows you to enable or disable the access to SNMP versions 1, 2 or 3.</p> <p>The default value is v1v2v3.</p> <p>Command mode: Global configuration</p>
<p>snmp-server view <1-128></p> <p>This command allows you to create different MIB views. To view command options, see page 222.</p> <p>Command mode: Global configuration</p>
<p>show snmp-server v3</p> <p>Displays the current SNMPv3 configuration.</p> <p>Command mode: All</p>

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 113. User Security Model Configuration Commands

Command Syntax and Usage
<p>snmp-server user <1-17> authentication-protocol {md5 sha none} authentication-password <password value></p> <p>This command allows you to configure the authentication protocol and password.</p> <p>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.</p> <p>MD5 authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility.</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>snmp-server user <1-17> name <1-32 characters></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>snmp-server user <1-17> privacy-protocol {aes des none} privacy-password <password value></p> <p>This command allows you to configure the type of privacy protocol and the privacy password.</p> <p>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.</p> <p>You can create or change the privacy password.</p> <p>Command mode: Global configuration</p>

Table 113. *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 114. *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 <code>vacmViewTreeFamilySubtree</code> and <code>vacmViewTreeFamilyMask</code> 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 <code>vacmViewTreeFamily</code> group entry. Command mode: Global configuration
show snmp-server v3 view <1-128> Displays the current <code>vacmViewTreeFamily</code> 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 115. *View-based Access Control Model Commands*

Command Syntax and Usage
<p>snmp-server access <1-32> level {noAuthNoPriv authNoPriv authPriv}</p> <p>Defines the minimum level of security required to gain access rights. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p>Command mode: Global configuration</p>
<p>snmp-server access <1-32> match {exact prefix}</p> <p>If the value is set to <code>exact</code>, then all the rows whose <code>contextName</code> exactly matches the prefix are selected. If the value is set to <code>prefix</code> then the all the rows where the starting octets of the <code>contextName</code> exactly match the prefix are selected.</p> <p>Command mode: Global configuration</p>
<p>snmp-server access <1-32> name <1-32 characters></p> <p>Defines the name of the group.</p> <p>Command mode: Global configuration</p>
<p>snmp-server access <1-32> notify-view <1-32 characters></p> <p>Defines a notify view name that allows you notify access to the MIB view.</p> <p>Command mode: Global configuration</p>
<p>snmp-server access <1-32> prefix <1-32 characters></p> <p>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 <code>contextName</code>.</p> <p>Command mode: Global configuration</p>
<p>snmp-server access <1-32> read-view <1-32 characters></p> <p>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.</p> <p>Command mode: Global configuration</p>

Table 115. *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 116. *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 221 . 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 221 : 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 117. *SNMPv3 Community Table Configuration Commands*

Command Syntax and Usage
<p>snmp-server community <1-16> index <1-32 characters></p> <p>Allows you to configure the unique index value of a row in this table.</p> <p>Command string: Global configuration</p>
<p>snmp-server community <1-16> name <1-32 characters></p> <p>Defines the user name as defined in the following command on page 221:</p> <p>snmp-server user <1-17> name <1-32 characters></p> <p>Command string: Global configuration</p>
<p>snmp-server community <1-16> tag <1-255 characters></p> <p>Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap.</p> <p>Command mode: Global configuration</p>
<p>snmp-server community <1-16> user-name <1-32 characters></p> <p>Defines a readable string that represents the corresponding value of an SNMP community name in a security model.</p> <p>Command mode: Global configuration</p>
<p>no snmp-server community <1-16></p> <p>Deletes the community table entry.</p> <p>Command mode: Global configuration</p>
<p>show snmp-server v3 community <1-16></p> <p>Displays the community table configuration.</p> <p>Command mode: All</p>

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 118. Target Address Table Configuration Commands

Command Syntax and Usage
<p>snmp-server target-address <1-16> {address address6} <IP address> name <1-32 characters></p> <p>Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-address <1-16> name <1-32 characters> {address address6} <transport IP address></p> <p>Configures a transport IPv4/IPv6 address that can be used in the generation of SNMP traps.</p> <p>Note: IPv6 addresses are not displayed in the configuration, but they do receive traps.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-address <1-16> parameters-name <1-32 characters></p> <p>Defines the name as defined in the following command on page 227: snmp-server target-parameters <1-16> name <1-32 characters></p> <p>Command mode: Global configuration</p>
<p>snmp-server target-address <1-16> port <port number></p> <p>Allows you to configure a transport address port that can be used in the generation of SNMP traps.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-address <1-16> taglist <1-255 characters></p> <p>Allows you to configure a list of tags that are used to select target addresses for a particular operation.</p> <p>Command mode: Global configuration</p>
<p>no snmp-server target-address <1-16></p> <p>Deletes the Target Address Table entry.</p> <p>Command mode: Global configuration</p>
<p>show snmp-server v3 target-address <1-16></p> <p>Displays the current Target Address Table configuration.</p> <p>Command mode: All</p>

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 119. Target Parameters Table Configuration Commands

Command Syntax and Usage
<p>snmp-server target-parameters <1-16> level {noAuthNoPriv authNoPriv authPriv}</p> <p>Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level <code>noAuthNoPriv</code> means that the SNMP message will be sent without authentication and without using a privacy protocol. The level <code>authNoPriv</code> means that the SNMP message will be sent with authentication but without using a privacy protocol. The <code>authPriv</code> means that the SNMP message will be sent both with authentication and using a privacy protocol.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-parameters <1-16> message {snmpv1 snmpv2c snmpv3}</p> <p>Allows you to configure the message processing model that is used to generate SNMP messages.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-parameters <1-16> name <1-32 characters></p> <p>Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-parameters <1-16> security {usm snmpv1 snmpv2}</p> <p>Allows you to select the security model to be used when generating the SNMP messages.</p> <p>Command mode: Global configuration</p>
<p>snmp-server target-parameters <1-16> user-name <1-32 characters></p> <p>Defines the name that identifies the user in the USM table (page 221) on whose behalf the SNMP messages are generated using this entry.</p> <p>Command mode: Global configuration</p>

Table 119. *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 120. *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 121. *System Access Configuration Commands*

Command Syntax and Usage
<p>[no] access snmp {read-only read-write} Enables or disables read-only/write-read SNMP access. Command mode: Global configuration</p>
<p>[no] access telnet enable Enables or disables Telnet access. The default settings is disabled. Command mode: Global configuration</p>
<p>[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</p>
<p>[default] access tftp-port [<1-65535>] Sets the TFTP port for the switch. The default is port 69. Command mode: Global configuration</p>
<p>access user administrator-password Sets the administrator (admin) password. The administrator has complete access to all menus, information, and configuration commands on the SI4093, 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</p>
<p>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</p>

Table 121. *System Access Configuration Commands (continued)*

Command Syntax and Usage
<p>access user user-password</p> <p>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.</p> <p>This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Note: To disable the user account, set the password to null (no password).</p> <p>Command Mode: Global configuration</p>
<p>show access</p> <p>Displays the current system access parameters.</p> <p>Command mode: All</p>

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 122. Management Network Configuration Commands

Command Syntax and Usage
<p>[no] access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length></p> <p>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.</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>access management-network <mgmt network IPv4 address> <mgmt network mask> {snmp-ro snmp-rw}</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>no access management-network {snmp-ro snmp-rw}</p> <p>Clears the IPv4 SNMP read-only or SNMP read/write access control list for management purposes.</p> <p>Command mode: Global configuration</p>
<p>access management-network6 <mgmt network IPv6 address> <IPv6 prefix length> {snmp-ro snmp-rw}</p> <p>Adds a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed.</p> <p>Command mode: Global configuration</p>
<p>no access management-network6 {snmp-ro snmp-rw}</p> <p>Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes.</p> <p>Command mode: Global configuration</p>

Table 122. *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

NETCONF Configuration

This menu allows you to configure support for Network Configuration Protocol (NETCONF), which provides mechanisms to install, manipulate, and delete the configuration of network devices. NETCONF is described in RFC 4741.

Table 123. *NETCONF Configuration Options*

Command Syntax and Usage
[no] access netconf enable Enables or disables NETCONF access to the switch. Command mode: Global configuration
access netconf timeout <30-3600> Configures the timeout value for NETCONF sessions, in seconds. The default value is 300 seconds. Command mode: Global configuration
default access netconf timeout Configures the timeout value for NETCONF sessions to the default value of 300 seconds. Commands mode: Global configuration
show access Displays the current configuration. Command mode: All

NETCONF over SSH Configuration

This menu allows you to enable NETCONF access over Secure Shell (SSH). NETCONF over SSH is described in RFC 4742.

Table 124. *NETCONF over SSH Configuration Options*

Command Syntax and Usage
[no] access netconf ssh enable Enables or disables NETCONF access over SSH. Command mode: Global configuration
access netconf ssh port <TCP port number> Configures the TCP port used for NETCONF. The default port number is 830. Command mode: Global configuration
default access netconf ssh port Configures the TCP port used for NETCONF to the default port number of 830. Command mode: Global configuration

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 125. *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 SI4093, including the ability to change both the user and administrator passwords. Note: Access includes “oper” functions. Command mode: Global configuration

Table 125. *User Access Control Configuration Commands*

Command Syntax and Usage
<p>access user operator-password <1-128 characters></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>access user user-password <1-128 characters></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>access user eject {<user name> <session ID>}</p> <p>Ejects the specified user from the SI4093.</p> <p>Command mode: Global configuration</p>
<p>clear line <1-12></p> <p>Ejects the user with the corresponding session ID from the SI4093.</p> <p>Command mode: All except User EXEC</p>
<p>show access user</p> <p>Displays the current user status.</p> <p>Command mode: All</p>

System User ID Configuration

The following table describes user ID configuration commands.

Table 126. *User ID Configuration Commands*

Command Syntax and Usage
<p>[no] access user <1-20> enable</p> <p>Enables or disables the user ID.</p> <p>Command mode: Global configuration</p>
<p>access user <1-20> level {user operator administrator}</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>access user <1-20> name <1-8 characters></p> <p>Defines the user name of maximum eight characters.</p> <p>Command mode: Global configuration</p>

Table 126. *User ID Configuration Commands*

Command Syntax and Usage
access user <1-20> password Sets the user (<i>user</i>) 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 127. *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

Table 127. *Strong Password Configuration Commands*

Command Syntax and Usage
<p>access user strong-password faillog <1-255></p> <p>Configures the number of failed login attempts allowed before a security notification is logged.</p> <p>The default value is 3.</p> <p>Command mode: Global configuration</p>
<p>[no] access user strong-password lockout</p> <p>Enables or disables account lockout after a specified number of failed login attempts.</p> <p>The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<p>access user strong-password warning <1-365></p> <p>Configures the number of days before password expiration, that a warning is issued to users.</p> <p>The default value is 15.</p> <p>Command mode: Global configuration</p>
<p>show access user strong-password</p> <p>Displays the current Strong Password configuration.</p> <p>Command mode: All</p>

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 128. *Custom DST Configuration Commands*

Command Syntax and Usage
<p>[no] system custom-dst enable</p> <p>Enables or disables the Custom Daylight Saving Time settings.</p> <p>Command mode: Global configuration</p>
<p>system custom-dst start-rule <WDDMMhh></p> <p>Configures the start date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)</p> <p>D = day of the week (01-07, where 01 is Monday)</p> <p>MM = month (1-12)</p> <p>hh = hour (0-23)</p> <p>Note: Week 5 is always considered to be the last week of the month.</p> <p>Command mode: Global configuration</p>
<p>system custom-dst end-rule <WDDMMhh></p> <p>Configures the end date for custom DST, as follows:</p> <p>WDDMMhh</p> <p>W = week (0-5, where 0 means use the calendar date)</p> <p>D = day of the week (01-07, where 01 is Monday)</p> <p>MM = month (1-12)</p> <p>hh = hour (0-23)</p> <p>Note: Week 5 is always considered to be the last week of the month.</p> <p>Command mode: Global configuration</p>
<p>show custom-dst</p> <p>Displays the current Custom DST configuration.</p> <p>Command mode: All</p>

Port Configuration

Use the Port Configuration commands to configure settings for switch ports (INTx) and (EXTx). If you are configuring management ports (MGT1), see [“Management Port Configuration” on page 250](#).

Table 129. *Port Configuration Commands*

Command Syntax and Usage
<p>interface port <port alias or number></p> <p>Enter Interface port mode.</p> <p>Command mode: Global configuration</p>
<p>description <1-64 characters></p> <p>Sets a description for the port. The assigned port name appears next to the port description on some information and statistics screens.</p> <p>The default is set to the port number.</p> <p>Command mode: Interface port</p>
<p>dot1p <0-7></p> <p>Configures the port's 802.1p priority level.</p> <p>Command mode: Interface port</p>
<p>[no] dscp-marking</p> <p>Enables or disables DSCP re-marking on a port.</p> <p>Command mode: Interface port</p>
<p>[no] flood-blocking</p> <p>Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.</p> <p>Command mode: Interface port</p>
<p>[no] learning</p> <p>Enables or disables FDB learning on the port.</p> <p>Command mode: Interface port</p>
<p>port-channel min-links <1-16></p> <p>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.</p> <p>Command mode: Interface port</p>
<p>[no] reflective-relay force</p> <p>Enables or disables constraint to always keep reflective relay active.</p> <p>The default setting is disabled.</p> <p>Command mode: Interface port</p>

Table 129. Port Configuration Commands (continued)

Command Syntax and Usage
<p>[no] rmon</p> <p>Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.</p> <p>Command mode: Interface port</p>
<p>shutdown</p> <p>Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to “Temporarily Disabling a Port” on page 244.)</p> <p>Command mode: Interface port</p>
<p>no shutdown</p> <p>Enables the port.</p> <p>Command mode: Interface port</p>
<p>[no] storm-control broadcast level rate <0-2097151></p> <p>Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets.</p> <p>Command mode: Interface port</p>
<p>[no] storm-control multicast level rate <0-2097151></p> <p>Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets.</p> <p>Command mode: Interface port</p>
<p>[no] storm-control unicast level rate <0-2097151></p> <p>Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets.</p> <p>Command mode: Interface port</p>
<p>switchport mode {access trunk private-vlan}</p> <p>Configures the port’s trunking mode:</p> <ul style="list-style-type: none"> 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 <p>The default mode is access.</p> <p>Note: When switching from access to trunk mode, the port inherits the access VLAN as the trunk Native-VLAN.</p> <p>Note: When switching from trunk to access mode, the port inherits the trunk Native-VLAN as the access VLAN.</p> <p>Command mode: Interface port/Interface portchannel</p>

Table 129. Port Configuration Commands (continued)

Command Syntax and Usage
<p>switchport trunk allowed vlan <VLAN ID range></p> <p>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.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>switchport trunk allowed vlan {add remove} <VLAN ID range></p> <p>Updates the associated VLANs in trunk mode.</p> <ul style="list-style-type: none"> 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. <p>Command mode: Interface port/Interface portchannel</p>
<p>switchport trunk allowed vlan {all none}</p> <p>Updates the associated VLANs in trunk mode.</p> <ul style="list-style-type: none"> 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. <p>Command mode: Interface port/Interface portchannel</p>
<p>no switchport trunk allowed vlan</p> <p>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.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>switchport trunk native vlan <1-4094></p> <p>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.</p> <p>Default value is 1 for data ports and 4095 for the management port.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>switchport access vlan <1-4094></p> <p>Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically.</p> <p>Default value is 1 for data ports and 4095 for the management port.</p> <p>Command mode: Interface port/Interface portchannel</p>

Table 129. Port Configuration Commands (continued)

Command Syntax and Usage
<p>no switchport access vlan</p> <p>Resets the access VLAN to its default value.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>[no] switchport private-vlan mapping <primary VLAN></p> <p>Enables or disables a private VLAN promiscuous port to/from a primary VLAN.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>[no] switchport private-vlan host-association <primary VLAN> <secondary VLAN></p> <p>Adds or removes a private VLAN host port to/from a secondary VLAN.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>[no] tagpvid-ingress</p> <p>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.</p> <p>The default setting is disabled.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>unicast-bandwidth <10-100></p> <p>Configures the allocated bandwidth percentage for unicast traffic on the port. The remaining bandwidth is automatically allocated to multicast traffic.</p> <p>The default value is 50.</p> <p>Command mode: Interface port</p>
<p>unicast-bandwidth global <10-100></p> <p>Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic.</p> <p>The default value is 50.</p> <p>Note: This applies to all ports.</p> <p>Command mode: Interface port</p>

Table 129. *Port Configuration Commands (continued)*

Command Syntax and Usage
<p>[no] vlan dot1q tag native</p> <p>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.</p> <p>The default setting is disabled.</p> <p>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.</p> <p>Command mode: Global configuration/Interface port/Interface portchannel</p>
<p>show interface port <i><port alias or number></i></p> <p>Displays current port parameters.</p> <p>Command mode: All</p>

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 130. *Port Error Disable Commands*

Command Syntax and Usage
<p>[no] errdisable link-flap enable</p> <p>Enables or disables Link Flap Dampening on the port. For more information, see “Link Flap Dampening Configuration” on page 200.</p> <p>Command mode: Interface port</p>
<p>[no] errdisable recovery</p> <p>Enables or disables automatic error-recovery for the port.</p> <p>The default setting is enabled.</p> <p>Note: Error-recovery must be enabled globally before port-level commands become active.</p> <p>Command mode: Interface port</p>
<p>show interface port <port alias or number> errdisable</p> <p>Displays current port Error Disable parameters.</p> <p>Command mode: All</p>

Port Link Configuration

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

Table 131. *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: <ul style="list-style-type: none">– 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 (EXTx) the default setting is <code>no flow control</code> , and for internal ports (INTx) 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: <ul style="list-style-type: none">– 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 4093# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the SI4093 System Interconnect Module is reset. See the [“Operations Commands” on page 355](#) for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 132. *Port UDLD Configuration Commands*

Command Syntax and Usage
<p>[no] udld</p> <p>Enables or disables UDLD on the port.</p> <p>Command mode: Interface port</p>
<p>[no] udld aggressive</p> <p>Configures the UDLD mode for the selected port, as follows:</p> <ul style="list-style-type: none">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. <p>Command mode: Interface port</p>
<p>show interface port <port number> udld</p> <p>Displays current port UDLD parameters.</p> <p>Command mode: All</p>

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 133. *Port OAM Configuration Commands*

Command Syntax and Usage
<p>oam [passive]</p> <p>Configures the OAM discovery mode, as follows:</p> <ul style="list-style-type: none">o Passive: This port allows its peer link to initiate OAM discovery. <p>If OAM determines that the port is in an anomalous condition, the port is disabled.</p> <p>Command mode: Interface port</p>
<p>no oam [passive]</p> <p>Disables OAM discovery on the port.</p> <p>Command mode: Interface port</p>
<p>show interface port <port number> oam</p> <p>Displays current port OAM parameters.</p> <p>Command mode: All</p>

Port ACL Configuration

The following table describes port ACL configuration commands.

Table 134. *Port ACL/QoS Configuration Commands*

Command Syntax and Usage
<p>[no] access-control group <1-256> Adds or removes the specified ACL group. You can add multiple ACL groups to a port. Command mode: Interface port</p>
<p>[no] access-control list <1-256> Adds or removes the specified ACL. You can add multiple ACLs to a port. Command mode: Interface port</p>
<p>[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</p>
<p>show interface port <port alias or number> access-control Displays current ACL QoS parameters. Command mode: All</p>

Port WRED Configuration

These commands allow you to configure Weighted Random Early Detection (WRED) parameters for a selected port. For global WRED configuration, see [“Weighted Random Early Detection Configuration” on page 255](#).

Table 135. *Port WRED Options*

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

Port WRED Transmit Queue Configuration

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

Table 136. Port WRED Transmit Queue Options

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

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 137. *Management Port Configuration Commands*

Command Syntax and Usage
<p>[no] auto Enables or disables auto-negotiation on the port. Command mode: Interface port</p>
<p>duplex {full half auto} Sets the operating mode. The choices include: – Full-duplex – Half-duplex – Auto — for auto negotiation (default) Command mode: Interface port</p>
<p>shutdown Disables the port. Command mode: Interface port</p>
<p>no shutdown Enables the port. Command mode: Interface port</p>
<p>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</p>
<p>show interface port <port alias or number> Displays current port parameters. Command mode: All</p>

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 SI4093 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 138. 802.1p Configuration Commands

Command Syntax and Usage
<p>qos transmit-queue mapping <priority (0-7)> <COSq number></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>qos transmit-queue weight-cos <COSq number> <weight (0-15)></p> <p>Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-1), followed by the scheduling weight (0-15).</p> <p>Command mode: Global configuration</p>
<p>qos unicast-bandwidth <10-90></p> <p>Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic.</p> <p>The default value is 50.</p> <p>Note: This applies to all ports.</p> <p>Command mode: All</p>
<p>show qos transmit-queue</p> <p>Displays the current 802.1p parameters.</p> <p>Command mode: All</p>

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 139. *DSCP Configuration Commands*

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

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 140. *CoPP Commands*

Command Syntax and Usage
<p>qos protocol-packet-control packet-queue-map <i><packet queue number (0-47)> <packet type></i></p> <p>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:</p> <ul style="list-style-type: none"> – 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) – ecp (ECP 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) <p>Command mode: Global configuration</p>
<p>no qos protocol-packet-control packet-queue-map <i><packet type></i></p> <p>Clears the selected packet type from its associated packet queue.</p> <p>Command mode: Global configuration</p>
<p>qos protocol-packet-control rate-limit-packet-queue <i><packet queue number (0-47)> <1-10000></i></p> <p>Configures the number of packets per second allowed for each packet queue.</p> <p>Command mode: Global configuration</p>
<p>no qos protocol-packet-control rate-limit-packet-queue <i><packet queue number (0-47)></i></p> <p>Clears the packet rate configured for the selected packet queue.</p> <p>Command mode: Global configuration</p>

Table 140. *CoPP Commands*

Command Syntax and Usage
show qos protocol-packet-control information protocol Displays of mapping of protocol packet types to each packet queue number. The status indicates whether the protocol is running or not running. Command mode: All
show qos protocol-packet-control information queue Displays the packet rate configured for each packet queue. Command mode: All

Weighted Random Early Detection Configuration

Weighted Random Early Detection (WRED) provides congestion avoidance by pre-emptively dropping packets before a queue becomes full. SI4093 implementation of WRED defines TCP and non-TCP traffic profiles on a per-port, per COS queue basis. For each port, you can define a transmit-queue profile with thresholds that define packet-drop probability.

These commands allow you to configure global WRED parameters. For port WRED commands, see [“Port WRED Configuration” on page 248](#).

Table 141. *WRED Configuration Options*

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

WRED Transmit Queue Configuration

The following table displays WRED Transmit Queue configuration commands.

Table 142. *WRED Transmit Queue Options*

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

Table 142. WRED Transmit Queue Options

Command Syntax and Usage
<p>qos random-detect transmit-queue <0-7> non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)> Configures the WRED thresholds for non-TCP traffic. Command mode: Global configuration</p>
<p>no qos random-detect transmit-queue <0-7> {tcp non-tcp} Clears the specified WRED threshold value. Command mode: Global configuration</p>

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 247](#).

Table 143. *General ACL Configuration Commands*

Command Syntax and Usage
[no] access-control group <1-256> Configures an ACL Group. To view command options, see page 271 . Command mode: Global configuration
[no] access-control list <1-256> Configures an Access Control List. To view command options, see page 258 . Command mode: Global configuration
[no] access-control list6 <1-128> Configures an IPv6 Access Control List. To view command options, see page 263 . 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 144. *ACL Configuration Commands*

Command Syntax and Usage
<p>access-control list <1-256> action {permit deny} set-priority <0-7>}</p> <p>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).</p> <p>Command mode: Global configuration</p>
<p>[no] access-control list <1-256> egress-port port <port alias or number></p> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control list <1-256> statistics</p> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p>
<p>default access-control list <1-256></p> <p>Resets the ACL parameters to their default values.</p> <p>Command mode: Global configuration</p>
<p>show access-control list <1-256></p> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p>
<p>[no] access-control list6 <1-128></p> <p>Configures an IPv6 Access Control List. To view command options, see page 263.</p> <p>Command mode: Global configuration</p>

Ethernet Filtering Configuration

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

Table 145. *Ethernet Filtering Configuration Commands*

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

IPv4 Filtering Configuration

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

Table 146. *IP version 4 Filtering Configuration Commands*

Command Syntax and Usage															
<p>[no] access-control list <1-256> ipv4 destination-ip-address <IP address> [<i><IP mask></i>]</p> <p>Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.</p> <p>Command mode: Global configuration</p>															
<p>[no] access-control list <1-256> ipv4 source-ip-address <IP address> [<i><IP mask></i>]</p> <p>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.</p> <p>Command mode: Global configuration</p>															
<p>[no] access-control list <1-256> ipv4 protocol <0-255></p> <p>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.</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>icmp</td> </tr> <tr> <td>2</td> <td>igmp</td> </tr> <tr> <td>6</td> <td>tcp</td> </tr> <tr> <td>17</td> <td>udp</td> </tr> <tr> <td>89</td> <td>ospf</td> </tr> <tr> <td>112</td> <td>vrrp</td> </tr> </tbody> </table> <p>Command mode: Global configuration</p>	Number	Name	1	icmp	2	igmp	6	tcp	17	udp	89	ospf	112	vrrp	
Number	Name														
1	icmp														
2	igmp														
6	tcp														
17	udp														
89	ospf														
112	vrrp														
<p>[no] access-control list <1-256> ipv4 type-of-service <0-255></p> <p>Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.</p> <p>Command mode: Global configuration</p>															
<p>default access-control list <1-256> ipv4</p> <p>Resets the IPv4 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>															
<p>show access-control list <1-256> ipv4</p> <p>Displays the current IPv4 parameters.</p> <p>Command mode: All</p>															

TCP/UDP Filtering Configuration

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

Table 147. *TCP/UDP Filtering Configuration Commands*

Command Syntax and Usage																													
<p>[no] access-control list <1-256> tcp-udp source-port <1-65535> [<mask (0xFFFF)>]</p> <p>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:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p>Command mode: Global configuration</p>	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	
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																												
<p>[no] access-control list <1-256> tcp-udp destination-port <1-65535> [<mask (0xFFFF)>]</p> <p>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 <code>source-port</code> above.</p> <p>Command mode: Global configuration</p>																													
<p>[no] access-control list <1-256> tcp-udp flags <value (0x0-0x3f)> [<mask (0x0-0x3f)>]</p> <p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p>																													
<p>default access-control list <1-256> tcp-udp</p> <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>																													
<p>show access-control list <1-256> tcp-udp</p> <p>Displays the current TCP/UDP Filtering parameters.</p> <p>Command mode: All</p>																													

Packet Format Filtering Configuration

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

Table 148. *Packet Format Filtering Configuration Commands*

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

ACL IPv6 Configuration

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

Table 149. *IPv6 ACL Options*

Command Syntax and Usage
<p>access-control list6 <1-128> action {permit deny} [set-priority <0-7>}]</p> <p>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).</p> <p>Command mode: Global configuration</p>
<p>[no] access-control list6 <1-128> egress-port port <port alias or number></p> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control list6 <1-128> statistics</p> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p>
<p>default access-control list6 <1-128></p> <p>Resets the ACL parameters to their default values.</p> <p>Command mode: Global configuration</p>
<p>show access-control list6 <1-128></p> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p>

IPv6 Filtering Configuration

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

Table 150. *IP version 6 Filtering Options*

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

IPv6 TCP/UDP Filtering Configuration

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

Table 151. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage																													
<p>[no] access-control list6 <1-128> tcp-udp source-port <1-65535> [<mask (0xFFFF)>]</p> <p>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:</p> <table border="1"> <thead> <tr> <th>Number</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>20</td><td>ftp-data</td></tr> <tr><td>21</td><td>ftp</td></tr> <tr><td>22</td><td>ssh</td></tr> <tr><td>23</td><td>telnet</td></tr> <tr><td>25</td><td>smtp</td></tr> <tr><td>37</td><td>time</td></tr> <tr><td>42</td><td>name</td></tr> <tr><td>43</td><td>whois</td></tr> <tr><td>53</td><td>domain</td></tr> <tr><td>69</td><td>tftp</td></tr> <tr><td>70</td><td>gopher</td></tr> <tr><td>79</td><td>finger</td></tr> <tr><td>80</td><td>http</td></tr> </tbody> </table> <p>Command mode: Global configuration</p>	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	
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																												
<p>[no] access-control list6 <1-128> tcp-udp destination-port <1-65535> [<mask (0xFFFF)>]</p> <p>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.</p> <p>Command mode: Global configuration</p>																													
<p>[no] access-control list6 <1-128> tcp-udp flags <value (0x0-0x3f)> [<mask (0x0-0x3f)>]</p> <p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p>																													
<p>default access-control list6 <1-128> tcp-udp</p> <p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>																													
<p>show access-control list6 <1-128> tcp-udp</p> <p>Displays the current TCP/UDP Filtering parameters.</p> <p>Command mode: All</p>																													

VMAP Configuration

A VLAN Map is an Access Control List (ACL) that can be assigned to a VLAN or a VM group instead of a port. In a virtualized environment where Virtual Machines move between physical servers, VLAN Maps allow you to create traffic filtering and metering policies associated with a VM's VLAN.

For more information about VLAN Map configuration commands, see [“Access Control List Configuration” on page 258](#).

For more information about assigning VLAN Maps to a VLAN, see [“VLAN Configuration” on page 303](#).

For more information about assigning VLAN Maps to a VM group, see [“VM Group Configuration” on page 336](#).

[Table 152](#) lists the general VMAP configuration commands.

Table 152. *VMAP Configuration Commands*

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

Table 152. VMAP Configuration Commands (continued)

Command Syntax and Usage
<p>[no] access-control vmap <1-128> ethernet ethernet-type {<0x600-0xFFF> any arp rarp ip ipv6 mpls}</p> <p>Enables or disables filtering of VMAP statistics collection based on the encapsulated protocol:</p> <ul style="list-style-type: none"> o <0x600-0xFFF> filters Ethernet frames with the specified EtherType o any filters all frames o arp filters Address Resolution Protocol frames o rarp filters Reverse Address Resolution Protocol frames o ip filters Internet Protocol version 4 frames o ipv6 filters Internet Protocol version 6 frames o mpls filters Multiprotocol Label Switching frames <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ethernet priority <0-7></p> <p>Enables or disables filtering of VMAP statistics collection based on the IEEE 802.1Q priority code point value.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ethernet vlan <1-4094></p> <p>Enables or disables filtering of VMAP statistics collection based on VLAN ID.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ipv4 destination-ip-address <IPv4 address> <IPv4 mask></p> <p>Enables or disables filtering of VMAP statistics collection based on destination IP address.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ipv4 source-ip-address <IPv4 address> <IPv4 mask></p> <p>Enables or disables filtering of VMAP statistics collection based on source IP address.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ipv4 protocol <0-255></p> <p>Enables or disables filtering of VMAP statistics collection based on protocol.</p> <p>Command mode: Global configuration</p>
<p>[no] access-control vmap <1-128> ipv4 type-of-service <0-255></p> <p>Enables or disables filtering of VMAP statistics collection based on type of service.</p> <p>Command mode: Global configuration</p>

Table 152. VMAP Configuration Commands (continued)

Command Syntax and Usage
access-control vmap <1-128> meter action {drop pass} Sets ACL port metering to drop or pass out-of-profile traffic. Command mode: Global configuration
access-control vmap <1-128> meter committed-rate <64-4000000> Sets the ACL port metering control rate in kilobits per second. Command mode: Global configuration
[no] access-control vmap <1-128> meter enable Enables or disables ACL port metering. Command mode: All except User EXEC
access-control vmap <1-128> meter maximum-burst-size <32-4096> Sets the ACL port metering maximum burst size in kilobytes. The following eight values are allowed: <ul style="list-style-type: none">– 32– 64– 128– 256– 512– 1024– 2048– 4096 Command mode: Global configuration
access-control vmap <1-128> mirror port <port> Sets the specified port as the mirror target. Command mode: Global configuration
no access-control vmap <1-128> mirror Turns off ACL mirroring. Command mode: Global configuration
access-control vmap <1-128> packet-format ethernet {ethernet-type2 llc snap} Sets to filter the specified ethernet packet format type. Command mode: Global configuration
access-control vmap <1-128> packet-format ip {ipv4 ipv6} Sets to filter the specified IP packet format type. Command mode: Global configuration

Table 152. VMAP Configuration Commands (continued)

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

Table 152. *VMAP Configuration Commands (continued)*

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

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 153. *ACL Group Configuration Commands*

Command Syntax and Usage
[no] access-control group <1-256> list <1-256> Adds or removes the selected ACL to/from the ACL group. Command mode: Global configuration
[no] access-control group <1-256> list6 <1-128> Adds or removes the selected IPv6 ACL to/from the ACL group. Command mode: Global configuration
show access-control group <1-256> Displays the current ACL group parameters. Command mode: All

ACL Metering Configuration

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

Table 154. *ACL Metering Configuration Commands*

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

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 155. *ACL Re-Marking Configuration Commands*

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

Re-Marking In-Profile Configuration

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

Table 156. *ACL Re-Mark In-Profile Commands*

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

Re-Marking Out-Profile Configuration

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

Table 157. *ACL Re-Mark Out-of-Profile Commands*

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

IPv6 Re-Marking Configuration

You can choose to re-mark IPv6 header data for the selected ACL. You can configure different re-mark values, based on whether packets fall within or outside the ACL metering profile.

Table 158. *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 159. *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 160. *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 SI4093, 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 161. *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 162. *Port-Based Port Mirroring Configuration Commands*

Command Syntax and Usage
<p>port-mirroring monitor-port <i><port alias or number></i> mirroring-port <i><port alias or number></i> {in out both}</p> <p>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:</p> <p>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.</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>no port-mirroring monitor-port <i><port alias or number></i> mirroring-port <i><port alias or number></i></p> <p>Removes the mirrored port.</p> <p>Command mode: Global configuration</p>
<p>show port-mirroring</p> <p>Displays the current settings of the monitoring port.</p> <p>Command mode: All</p>

Layer 2 Configuration

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

Table 163. *Layer 2 Configuration Commands*

Command Syntax and Usage
vlan <VLAN number> Enter VLAN configuration mode. To view command options, see page 303 . 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 164. *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 165. *Static Multicast MAC Configuration Commands*

Command Syntax and Usage
<p>[no] mac-address-table multicast <MAC address> <VLAN number> <port alias or number></p> <p>Adds or deletes a permanent multicast FDB entry. You can list ports separated by a space, or enter a range of ports separated by a hyphen (-). For example:</p> <pre>mac-address-table multicast 01:00:00:23:3f:01 200 int1-int4</pre> <p>Command mode: Global configuration</p>
<p>no mac-address-table multicast all</p> <p>Deletes all permanent multicast FDB entries.</p> <p>Command mode: Global configuration</p>
<p>mac-address-table multicast reload</p> <p>Reloads all permanent multicast FDB entries.</p> <p>Command mode: Global configuration</p>
<p>show mac-address-table multicast</p> <p>Display the current permanent multicast FDB entries.</p> <p>Command mode: All</p>

Static FDB Configuration

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

Table 166. FDB Configuration Commands

Command Syntax and Usage
<p>mac-address-table static <MAC address> vlan <VLAN number> {port <port alias or number> portchannel <LAG number> adminkey <1-65535>}</p> <p>Adds a permanent FDB entry. Enter the MAC address using the following format, xx:xx:xx:xx:xx:xx.</p> <p>For example, 08:00:20:12:34:56.</p> <p>You can also enter the MAC address as follows: xxxxxxxxxxxx.</p> <p>For example, 080020123456.</p> <p>Command mode: Global configuration</p>
<p>no mac-address-table static <MAC address> <VLAN number></p> <p>Deletes a permanent FDB entry.</p> <p>Command mode: Global configuration</p>
<p>show mac-address-table</p> <p>Display current FDB configuration.</p> <p>Command mode: All</p>

LLDP Configuration

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

Table 167. *LLDP Configuration Commands*

Command Syntax and Usage
<p>[no] lldp enable</p> <p>Globally enables or disables LLDP. The default setting is enabled.</p> <p>Command mode: Global configuration</p>
<p>lldp holdtime-multiplier <2-10></p> <p>Configures the message hold time multiplier. The hold time is configured as a multiple of the message transmission interval. The default value is 4.</p> <p>Command mode: Global configuration</p>
<p>no lldp holdtime-multiplier</p> <p>Sets the message hold time multiplier to its default value of 4.</p> <p>Command mode: Global configuration</p>
<p>lldp refresh-interval <5-32768></p> <p>Configures the message transmission interval, in seconds. The default value is 30.</p> <p>Command mode: Global configuration</p>
<p>no lldp refresh-interval</p> <p>Sets the message transmission interval to its default value of 30 seconds.</p> <p>Command mode: Global configuration</p>
<p>lldp reinit-delay <1-10></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>no lldp reinit-delay</p> <p>Sets the re-initialization delay interval to its default value of 2 seconds.</p> <p>Command mode: Global configuration</p>
<p>lldp transmission-delay <1-8192></p> <p>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.</p> <p>Command mode: Global configuration</p>

Table 167. *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 168. *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: <ul style="list-style-type: none">o Transmit onlyo Receive onlyo 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 169. *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 169. *Optional TLV Commands (continued)*

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

Link Aggregation Group (LAG) Configuration

Link Aggregation Groups (LAGs) can provide super-bandwidth connections between SI4093 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: 1-64
- LACP LAGs: 65-128

Up to 64 static LAGs can be configured on the SI4093, with the following restrictions:

- Any physical switch port can belong to no more than one LAG.
- Up to 16 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 65.

Table 170. LAG Configuration Commands

Command Syntax and Usage
portchannel <1-64> 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 <1-64> port <port alias or number> Removes a physical port or ports from the current LAG. Command mode: Global configuration
[no] portchannel <1-64> enable Enables or disables the current LAG. Command mode: Global configuration

Table 170. LAG Configuration Commands (continued)

Command Syntax and Usage
no portchannel <1-64> Removes the current LAG configuration. Command mode: Global configuration
show portchannel <1-64> 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 SI4093. LAG hash parameters are set globally for the SI4093. 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 171](#) combined with the hash parameters listed in [Table 173](#).

Table 171. *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 <code>disabled</code> . 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 <code>disabled</code> . 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 SI4093.

Table 172. 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 173. *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 174. *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 SI4093.

Table 175. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
<p>lacp system-priority <1-65535></p> <p>Defines the priority value for the SI4093. Lower numbers provide higher priority.</p> <p>The default value is 32768.</p> <p>Command mode: Global configuration</p>
<p>lacp timeout {short long}</p> <p>Defines the timeout period before invalidating LACP data from a remote partner. Choose <code>short</code> (3 seconds) or <code>long</code> (90 seconds).</p> <p>The default value is <code>long</code>.</p> <p>Note: It is recommended that you use a timeout value of <code>long</code>, to reduce LACPDU processing. If your SI4093's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static LAGs instead of LACP.</p> <p>Command mode: Global configuration</p>
<p>default lacp [system-priority timeout]</p> <p>Restores either the VFSM priority value, timeout period or both to their default values.</p> <p>Command mode: Global configuration</p>
<p>no lacp <1-65535></p> <p>Deletes a selected LACP LAG, based on its <i>admin key</i>. This command is equivalent to disabling LACP on each of the ports configured with the same <i>admin key</i>.</p> <p>Command mode: Global configuration</p>
<p>portchannel <LAG ID (65-128)> lacp key <1-65535></p> <p>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.</p> <p>Command mode: Global configuration</p>

Table 175. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
no portchannel <LAG ID (65-128)> 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 176. *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 <i>admin key</i> and <i>oper key</i> (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: <ul style="list-style-type: none">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 LACPDU s.o passive turns LACP on and set this port to passive. Passive ports do not initiate LACPDU s, but respond to LACPDU s 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 LACPDU s 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 176. *Link Aggregation Control Protocol Commands*

Command Syntax and Usage
<p>no lacp suspend-individual</p> <p>Sets the port in LACP individual state if it does not receive LACPDU's anymore.</p> <p>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.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>port-channel min-links <1-16></p> <p>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.</p> <p>Command mode: Interface port</p>
<p>default lacp [key mode priority suspend-individual]</p> <p>Restores the selected parameters to their default values.</p> <p>Command mode: Interface port/Interface portchannel</p>
<p>show interface port <port alias or number> lacp</p> <p>Displays the current LACP configuration for this port.</p> <p>Command mode: All</p>

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 177. *Layer 2 Failover Configuration Commands*

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

Failover Trigger Configuration

The following table displays Failover Trigger configuration commands.

Table 178. *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 179. *Auto Monitor Configuration Commands*

Command Syntax and Usage
[no] failover trigger <1-8> amon adminkey <1-65535> Adds or removes an LACP <i>admin key</i> to the Auto Monitor. LACP LAGs formed with this <i>admin key</i> 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 180. Failover Manual Monitor Port Commands

Command Syntax and Usage
<p>[no] failover trigger <1-8> mmon monitor adminkey <1-65535></p> <p>Adds or removes an LACP <i>admin key</i> to the Manual Monitor Port configuration. LACP LAGs formed with this <i>admin key</i> will be included in the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<p>[no] failover trigger <1-8> mmon monitor member <port alias or number></p> <p>Adds or removes the selected port to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<p>[no] failover trigger <1-8> mmon monitor portchannel <LAG number></p> <p>Adds or removes the selected LAG to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<p>show failover trigger <1-8></p> <p>Displays the current Failover settings.</p> <p>Command mode: All</p>

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 181. *Failover Manual Monitor Control Commands*

Command Syntax and Usage
<p>[no] failover trigger <1-8> mmon control adminkey <1-65535></p> <p>Adds or removes an LACP <i>admin key</i> to the Manual Monitor Control configuration. LACP LAGs formed with this <i>admin key</i> will be included in the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<p>[no] failover trigger <1-8> mmon control member <port alias or number></p> <p>Adds or removes the selected port to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<p>[no] failover trigger <1-8> mmon control portchannel <LAG number></p> <p>Adds or removes the selected LAG to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<p>[no] failover trigger <1-8> mmon control vmember <UFP vport(s)></p> <p>Adds or removes the selected Unified Fabric Port virtual port(s) to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<p>show failover trigger <1-8></p> <p>Displays the current Failover settings.</p> <p>Command mode: All</p>

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 182. *Hot Links Configuration Commands*

Command Syntax and Usage
<p>[no] hotlinks bpdu</p> <p>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).</p> <p>The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<p>[no] hotlinks enable</p> <p>Globally enables or disables Hot Links.</p> <p>Command mode: Global configuration</p>
<p>[no] hotlinks fdb-update</p> <p>Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface.</p> <p>The default value is disabled.</p> <p>Command mode: Global configuration</p>
<p>hotlinks fdb-update-rate <10-200></p> <p>Configures the FDB Update rate, in packets per second.</p> <p>Command mode: Global configuration</p>
<p>show hotlinks</p> <p>Displays current Hot Links parameters.</p> <p>Command mode: All</p>

Hot Links Trigger Configuration

The following table displays Hot Links Trigger configuration commands.

Table 183. 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 184. Hot Links Master Configuration Commands

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

Hot Links Backup Configuration

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

Table 185. Hot Links Backup Configuration Commands

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

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 S14093. VLANs can be assigned any number between 1 and 4094, except the reserved VLANs.

Table 186. *VLAN Configuration Commands*

<p>Command Syntax and Usage</p>
<p>vlan <VLAN number></p> <p>Enter VLAN configuration mode.</p> <p>Command mode: Global configuration</p>
<p>[no] cpu</p> <p>Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows:</p> <ul style="list-style-type: none"> 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. <p>The default setting is enabled.</p> <p>Note: If both flood and cpu are disabled, then the switch drops all unregistered IPMC traffic.</p> <p>Command mode: VLAN</p>
<p>[no] flood</p> <p>Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is enabled.</p> <p>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.</p> <p>Note: If both flood and cpu are disabled, then the switch drops all unregistered IPMC traffic.</p> <p>Command mode: VLAN</p>
<p>[no] management</p> <p>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.</p> <p>Command mode: VLAN</p>
<p>name <1-32 characters></p> <p>Assigns a name to the VLAN or changes the existing name.</p> <p>The default VLAN name is the first one.</p> <p>Command mode: VLAN</p>

Table 186. *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
[no] vmap <1-128> [extports intports] Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN. Command mode: VLAN
show vlan information Displays the current VLAN configuration. Command mode: All

Note: All ports must belong to at least one VLAN. Any 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 187. *Private VLAN Configuration Commands*

Command Syntax and Usage
<p>private-vlan association [add remove] <secondary VLAN list></p> <p>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:</p> <ul style="list-style-type: none">o add appends the secondary VLANs to the ones currently associatedo remove excludes the secondary VLANs from the ones currently associated <p>Command mode: VLAN</p>
<p>[no] private-vlan community</p> <p>Enables or disables the VLAN type as a community VLAN.</p> <p>Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.</p> <p>Command mode: VLAN</p>
<p>[no] private-vlan isolated</p> <p>Enables or disables the VLAN type as an isolated VLAN.</p> <p>The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.</p> <p>Command mode: VLAN</p>
<p>[no] private-vlan primary</p> <p>Enables or disables the VLAN type as a Primary VLAN.</p> <p>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.</p> <p>Command mode: VLAN</p>
<p>show vlan private-vlan [type]</p> <p>Displays private VLAN information. The type option lists only the VLAN type for each private VLAN: community, isolated or primary.</p> <p>Command mode: All</p>

Layer 3 Configuration

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

Table 188. *Layer 3 Configuration Commands*

Command Syntax and Usage
interface ip <interface number> Configures the IP Interface. The SI4093 supports up to 4 IP interfaces: 125, 126 for IPv6 and 127, 128 for IPv4. To view command options, see page 307 . Command mode: Global configuration
show layer3 Displays the current IP configuration. Command mode: All

IP Interface Configuration

The SI4093 supports up to 4 IP interfaces: 125, 126 for IPv6 and 127, 128 for IPv4. Each IP interface represents the SI4093 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 SI4093, use the management module interface to change the IP address of the switch.

Table 189. *IP Interface Configuration Commands*

Command Syntax and Usage
<p>interface ip <interface number></p> <p>Enter IP interface mode.</p> <p>Command mode: Global configuration</p>
<p>[no] enable</p> <p>Enables or disables this IP interface.</p> <p>Command mode: Interface IP</p>
<p>ip address <IP address> [<IP netmask>]</p> <p>Configures the IP address of the switch interface, using dotted decimal notation.</p> <p>Command mode: Interface IP</p>
<p>ip netmask <IP netmask></p> <p>Configures the IP subnet address mask for the interface, using dotted decimal notation.</p> <p>Command mode: Interface IP</p>
<p>[no] ip6host</p> <p>Enables or disables the IPv6 Host Mode on this interface.</p> <p>The default setting is disabled for data interfaces, and enabled for the management interface.</p> <p>Command mode: Interface IP</p>
<p>ipv6 address <IPv6 address> [enable]</p> <p>ipv6 address <IPv6 address> <IPv6 prefix length (1-128)> [enable]</p> <p>ipv6 address <IPv6 address> <IPv6 prefix length (1-128)> anycast [enable]</p> <p>Configures the IPv6 address of the switch interface, using hexadecimal format with colons.</p> <p>Command mode: Interface IP</p>
<p>ipv6 prefixlen <IPv6 prefix length (1-128)></p> <p>Configures the subnet IPv6 prefix length.</p> <p>The default value is 0.</p> <p>Command mode: Interface IP</p>

Table 189. *IP Interface Configuration Commands (continued)*

Command Syntax and Usage
<p>ipv6 secaddr6 address <IPv6 address> <IPv6 prefix length (1-128)> [anycast]</p> <p>Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.</p> <p>Command mode: Interface IP</p>
<p>no ipv6 secaddr6</p> <p>Removes the secondary IPv6 address of the switch interface.</p> <p>Command mode: Interface IP</p>
<p>[no] ipv6 unreachable</p> <p>Enables or disables sending of ICMP Unreachable messages. The default setting is enabled.</p> <p>Command mode: Interface IP</p>
<p>no interface ip <interface number></p> <p>Removes this IP interface.</p> <p>Command mode: Interface IP</p>
<p>show interface ip <interface number></p> <p>Displays the current interface settings.</p> <p>Command mode: All</p>

IPv6 Neighbor Discovery Configuration

The following table describes the IPv6 Neighbor Discovery Configuration commands.

Table 190. *IPv6 Neighbor Discovery Configuration Options*

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

Table 190. IPv6 Neighbor Discovery Configuration Options (continued)

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

Table 190. IPv6 Neighbor Discovery Configuration Options (continued)

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

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 191. *Default Gateway Configuration Commands*

Command Syntax and Usage
<p>ip gateway <3-4> address <IP address> [enable]</p> <p>Configures the IP address of the default IP gateway using dotted decimal notation. The enable option also enables the IP gateway for use.</p> <p>Command mode: Global configuration</p>
<p>[no] ip gateway <3-4> arp-health-check</p> <p>Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is disabled.</p> <p>Note: The arp option does not apply to management gateways.</p> <p>Command mode: Global configuration</p>
<p>[no] ip gateway <3-4> enable</p> <p>Enables or disables the gateway for use.</p> <p>Command mode: Global configuration</p>
<p>ip gateway <3-4> interval <0-60></p> <p>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.</p> <p>The default is 2.</p> <p>Command mode: Global configuration</p>
<p>ip gateway <3-4> retry <1-120></p> <p>Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts.</p> <p>The default is 8 attempts.</p> <p>Command mode: Global configuration</p>
<p>no ip gateway <3-4></p> <p>Deletes the gateway from the configuration.</p> <p>Command mode: Global configuration</p>
<p>show ip gateway <3-4></p> <p>Displays the current gateway settings.</p> <p>Command mode: All</p>

Network Filter Configuration

The following table displays Network Filter configuration commands.

Table 192. *IP Network Filter Configuration Commands*

Command Syntax and Usage
[no] ip match-address <1-256> enable Enables or disables the Network Filter configuration. Command mode: Global configuration
no ip match-address <1-256> Deletes the Network Filter configuration. Command mode: Global configuration
show ip match-address [<1-256>] Displays the current the Network Filter configuration. Command mode: All

IGMP Configuration

[Table 193](#) describes the commands used to configure basic IGMP parameters.

Table 193. *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 314](#)
- [“IGMPv3 Configuration” on page 315](#)
- [“IGMP Static Multicast Router Configuration” on page 318](#)
- [“IGMP Filtering Configuration” on page 316](#)
- [“IGMP Advanced Configuration” on page 319](#)

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 194 describes the commands used to configure IGMP Snooping.

Table 194. 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 195 describes the commands used to configure IGMP version 3.

Table 195. *IGMP version 3 Configuration Commands*

Command Syntax and Usage
<p>[no] ip igmp snoop igmpv3 enable</p> <p>Enables or disables IGMP version 3. The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<p>[no] ip igmp snoop igmpv3 exclude</p> <p>Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default setting is enabled.</p> <p>Command mode: Global configuration</p>
<p>ip igmp snoop igmpv3 sources <1-64></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>[no] ip igmp snoop igmpv3 v1v2</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>show ip igmp snoop igmpv3</p> <p>Displays the current IGMP v3 Snooping configuration.</p> <p>Command mode: All</p>

IGMP Filtering Configuration

Table 196 describes the commands used to configure an IGMP filter.

Table 196. IGMP Filtering Configuration Commands

Command Syntax and Usage
ip igmp profile <1-16> Configures the IGMP filter. To view command options, see page 316 . 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 197 describes the commands used to define an IGMP filter.

Table 197. 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 198 describes the commands used to configure a port for IGMP filtering.

Table 198. *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 199 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 199. 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 200 describes the commands used to configure advanced IGMP parameters.

Table 200. IGMP Advanced Configuration Commands

Command Syntax and Usage
<p>[no] ip igmp fastleave <VLAN number></p> <p>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.</p> <p>The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<p>ip igmp query-interval <1-600></p> <p>Sets the IGMP router query interval, in seconds.</p> <p>The default value is 125.</p> <p>Command mode: Global configuration</p>
<p>ip igmp robust <1-10></p> <p>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.</p> <p>The default value is 2.</p> <p>Command mode: Global configuration</p>
<p>[no] ip igmp rtralert</p> <p>Enables or disables the Router Alert option in IGMP messages.</p> <p>Command mode: Global configuration</p>
<p>ip igmp timeout <1-255></p> <p>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.</p> <p>The default value is 10.</p> <p>Command mode: Global configuration</p>

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`, `tracert`, and `tftp` commands.

Table 201. *Domain Name Service Commands*

Command Syntax and Usage
<p>[no] ip dns domain-name <string></p> <p>Sets the default domain name used by the switch.</p> <p>For example: mycompany.com</p> <p>Command mode: Global configuration</p>
<p>[no] ip dns primary-server <IP address></p> <p>You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation.</p> <p>Command mode: Global configuration</p>
<p>[no] ip dns secondary-server <IP address></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>[no] ip dns ipv6 primary-server <IP address></p> <p>You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons.</p> <p>Command mode: Global configuration</p>
<p>[no] ip dns ipv6 secondary-server <IP address></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>ip dns ipv6 request-version {ipv4 ipv6}</p> <p>Sets the protocol used for the first request to the DNS server, as follows:</p> <ul style="list-style-type: none">o IPv4o IPv6 <p>Command mode: Global configuration</p>
<p>show ip dns</p> <p>Displays the current Domain Name System settings.</p> <p>Command mode: All</p>

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateways 3 and 4 are used for management traffic.

[Table 202](#) describes the IPv6 Default Gateway Configuration commands.

Table 202. *IPv6 Default Gateway Configuration Commands*

Command Syntax and Usage
<p>ip gateway6 <3-4> address <IPv6 address> [enable]</p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>[no] ip gateway6 <3-4> enable</p> <p>Enables or disables the default gateway.</p> <p>Command mode: Global configuration</p>
<p>no ip gateway6 <3-4></p> <p>Deletes the default gateway.</p> <p>Command mode: Global configuration</p>
<p>show ipv6 gateway6 <3-4></p> <p>Displays the current IPv6 default gateway configuration.</p> <p>Command mode: All</p>

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 203. *IPv6 Path MTU Commands*

Command Syntax and Usage
<p>ip pmtu6 timeout {0 <10-100>}</p> <p>Sets the timeout value for Path MTU cache entries, in minutes. Enter 0 (zero) to set the timeout to infinity (no timeout).</p> <p>The default value is 10.</p> <p>Command mode: Global configuration</p>
<p>clear ipv6 pmtu</p> <p>Clears all entries in the Path MTU cache.</p> <p>Command mode: All Except User EXEC</p>
<p>show ipv6 pmtu</p> <p>Displays the current Path MTU configuration.</p> <p>Command mode: All</p>

Converged Enhanced Ethernet Configuration

Table 204 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 204. *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 205](#) describes the global ETS Priority Group configuration options.

Table 205. *Global ETS Priority Group Commands*

Command Syntax and Usage
<p>cee global ets priority-group pgid <0-7, 15> bandwidth <802.1p priority (0-7)> <bandwidth percentage (0, 10-100)></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>cee global ets priority-group pgid <0-7, 15> description <1-31 characters></p> <p>Enter text that describes this Priority Group.</p> <p>Command mode: Global configuration</p>
<p>no cee global ets priority-group <0-7, 15> description</p> <p>Removes the description for the specified Priority Group.</p> <p>Command mode: Global configuration</p>
<p>cee global ets priority-group pgid <0-7, 15> priority <0-7></p> <p>Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.</p> <p>Command mode: Global configuration</p>
<p>show cee global ets</p> <p>Displays the current global ETS Priority Group parameters.</p> <p>Command mode: All</p>
<p>show cee global ets priority-group <0-7, 15></p> <p>Displays the current global ETS Priority Group parameters.</p> <p>Command mode: All</p>

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 206 describes the global PFC Priority Group configuration options.

Table 206. *Global PFC Priority 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 207 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 207. Port 802.1p PFC Options

Command Syntax and Usage
<p>[no] cee port <port alias or number> pfc enable</p> <p>Enables or disables Priority Flow Control on the selected port.</p> <p>Command mode: Global configuration</p>
<p>cee port <port alias or number> pfc priority <0-7> description <1-31 characters></p> <p>Enter text to describe the priority value.</p> <p>Command mode: Global configuration</p>
<p>no cee port <port alias or number> pfc priority <0-7> description</p> <p>Deletes the description from the specified priority value.</p> <p>Command mode: Global configuration</p>
<p>[no] cee port <port alias or number> pfc priority <0-7> enable</p> <p>Enables or disables Priority Flow Control on the selected 802.1p priority.</p> <p>Note: PFC can be enabled on 802.1p priority 3 and one other priority only.</p> <p>Command mode: Global configuration</p>
<p>show cee port <port alias or number> pfc priority <0-7></p> <p>Displays the current 802.1p PFC parameters for the selected port.</p> <p>Command mode: All</p>
<p>show cee port <port alias or number> pfc</p> <p>Displays the current PFC parameters for the selected port.</p> <p>Command mode: All</p>

DCBX Port Configuration

Table 208 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 208. *Port DCBX Commands*

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

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 209](#) describes the FCoE configuration options.

Table 209. *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 210](#) describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 210. *Port FIP Snooping Commands*

Command Syntax and Usage
<p>fcoe fips port <port alias or number> fcf-mode [auto on off]</p> <p>Configures FCoE Forwarding (FCF) on the port, as follows:</p> <ul style="list-style-type: none">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. <p>Command mode: Global configuration</p>
<p>[no] fcoe fips port <port alias or number> enable</p> <p>Enables or disables FIP Snooping on the port.</p> <p>The default setting is enabled.</p> <p>Note: If IPv6 ACLs are assigned to the port, you cannot enable FCoE.</p> <p>Command mode: Global configuration</p>

Remote Monitoring Configuration

Remote Monitoring (RMON) allows you to monitor traffic flowing through the switch. The RMON MIB is described in RFC 1757.

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

- “RMON History Configuration” on page 330
- “RMON Event Configuration” on page 331
- “RMON Alarm Configuration” on page 332

RMON History Configuration

Table 211 describes the RMON History commands.

Table 211. *RMON History Commands*

Command Syntax and Usage
<p>rmon history <1-65535> interface-oid <1-127 characters></p> <p>Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows:</p> <p>1.3.6.1.2.1.2.2.1.1.x, where x is the ifIndex.</p> <p>Command mode: Global configuration</p>
<p>rmon history <1-65535> owner <1-127 characters></p> <p>Enter a text string that identifies the person or entity that uses this History index.</p> <p>Command mode: Global configuration</p>
<p>rmon history <1-65535> polling-interval <1-3600></p> <p>Configures the time interval over which the data is sampled for each bucket. The default value is 1800.</p> <p>Command mode: Global configuration</p>
<p>rmon history <1-65535> requested-buckets <1-65535></p> <p>Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved.</p> <p>The default value is 30.</p> <p>Note: The maximum number of buckets that can be granted is 50.</p> <p>Command mode: Global configuration</p>

Table 211. *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 212](#) describes the RMON Event commands.

Table 212. *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 213](#) describes the RMON Alarm commands.

Table 213. *RMON Alarm Commands*

Command Syntax and Usage
<p>rmon alarm <1-65535> alarm-type {rising falling either}</p> <p>Configures the alarm type as rising, falling, or either (rising or falling).</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> falling-crossing-index <1-65535></p> <p>Configures the falling alarm event index that is triggered when a falling threshold is crossed.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> falling-limit <-2147483647 - 214748364></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> interval <1-65535></p> <p>Configures the time interval over which data is sampled and compared with the rising and falling thresholds.</p> <p>The default value is 1800.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> oid <1-127 characters></p> <p>Configures an alarm MIB Object Identifier.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> owner <1-127 characters></p> <p>Enter a text string that identifies the person or entity that uses this alarm index.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> rising-crossing-index <1-65535></p> <p>Configures the rising alarm event index that is triggered when a rising threshold is crossed.</p> <p>Command mode: Global configuration</p>

Table 213. *RMON Alarm Commands (continued)*

Command Syntax and Usage
<p>rmon alarm <1-65535> rising-limit <-2147483647 - 2147483647></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>rmon alarm <1-65535> sample {abs delta}</p> <p>Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows:</p> <ul style="list-style-type: none">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. <p>Command mode: Global configuration</p>
<p>no rmon alarm <1-65535></p> <p>Deletes the selected RMON Alarm index.</p> <p>Command mode: Global configuration</p>
<p>show rmon alarm</p> <p>Displays the current RMON Alarm parameters.</p> <p>Command mode: All</p>

VMReady

Table 214 describes the VMReady configuration options.

Table 214. *VMReady Configuration Options*

Command Syntax and Usage
<p>[no] virt enable</p> <p>Enables or disables VMReady.</p> <p>Note: The no form of this command deletes all configured VM groups.</p> <p>Command mode: Global configuration</p>
<p>virt vmcheck</p> <p>Configures VM Check validation settings. For command options, see page 339.</p> <p>Command mode: Global configuration</p>
<p>virt vmgroup</p> <p>Configures VM Group settings. For command options, see page 336.</p> <p>Command mode: Global configuration</p>
<p>virt vmpolicy vmbwidth</p> <p>Configures VM Bandwidth management settings. For command options, see page 335.</p> <p>Command mode: Global configuration</p>
<p>virt vmprofile</p> <p>Configures VM Profile settings. For command options, see page 340.</p> <p>Command mode: Global configuration</p>
<p>virt vmrmisc</p> <p>Configures Miscellaneous VMready settings. For command options, see page 342.</p> <p>Command mode: Global configuration</p>
<p>virt vmware</p> <p>Configures VMware settings. For command options, see page 341.</p> <p>Command mode: Global configuration</p>
<p>show virt</p> <p>Displays the current virtualization parameters.</p> <p>Command mode: All</p>

VM Policy Bandwidth Management

Table 215 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 215. VM Bandwidth Management Options

Command Syntax and Usage
<p>[no] virt vmpolicy vmbwidth [<i><MAC address></i> <i><UUID></i> <i><name></i> <i><IP address></i> <i><index number></i>] bwctrl</p> <p>Enables or disables bandwidth control on the VM policy.</p> <p>Command mode: Global configuration</p>
<p>virt vmpolicy vmbwidth [<i><MAC address></i> <i><UUID></i> <i><name></i> <i><IP address></i> <i><index number></i>] rxrate <i><0-4000000></i> <i><max. burst (0-4096)></i></p> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>Command mode: Global configuration</p>
<p>virt vmpolicy vmbwidth [<i><MAC address></i> <i><UUID></i> <i><name></i> <i><IP address></i> <i><index number></i>] txrate <i><0-4000000></i> <i><max. burst (0-4096)></i> [<i><ACL number (1-256)></i>]</p> <p>The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.</p> <p>The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.</p> <p>The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.</p> <p>Command mode: Global configuration</p>
<p>no virt vmpolicy vmbwidth [<i><MAC address></i> <i><UUID></i> <i><name></i> <i><IP address></i> <i><index number></i>]</p> <p>Deletes the bandwidth management settings from this VM policy.</p> <p>Command mode: Global configuration</p>
<p>show virt vmpolicy vmbwidth [<i><MAC address></i> <i><UUID></i> <i><name></i> <i><IP address></i> <i><index number></i>]</p> <p>Displays the current VM bandwidth management parameters.</p> <p>Command mode: All</p>

VM Group Configuration

Table 216 describes the VM group configuration options. A VM group is a collection of members, such as VMs, ports, or LAGs. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 216. VM Group Commands

Command Syntax and Usage
<p>virt vmgroup <1-4096> cpu</p> <p>Enables or disables sending unregistered IPMC traffic to CPU.</p> <p>Command mode: Global configuration</p>
<p>virt vmgroup <1-4096> flood</p> <p>Enables or disables flooding unregistered IPMC traffic.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> key <1-65535></p> <p>Adds or removes an LACP <i>admin key</i> to the VM group. LACP LAGs formed with this <i>admin key</i> will be included in the VM group.</p> <p>Command mode: Global configuration</p>
<p>virt vmgroup <1-4096> optflood</p> <p>Enables or disables optimized flooding.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> port <port number or alias></p> <p>Adds or removes the selected port to the VM group.</p> <p>Note: A port can be added to a VM group only if no VMs on that port are members of the VM group.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> portchannel <LAG number></p> <p>Adds or removes the selected LAG to the VM group.</p> <p>Command mode: Global configuration</p>
<p>virt vmgroup <1-4096> profile <profile name (1-39 characters)></p> <p>Adds the selected VM profile to the VM group.</p> <p>Command mode: Global configuration</p>
<p>no virt vmgroup <1-4096> profile</p> <p>Removes the VM profile assigned to the VM group.</p> <p>Note: This command can only be used if the VM group is empty (only has the profile assigned).</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> tag</p> <p>Enables or disables VLAN tagging on ports in this VM group.</p> <p>Command mode: Global configuration</p>

Table 216. VM Group Commands (continued)

Command Syntax and Usage
<p>virt vmgroup <1-4096> validate [basic advanced]</p> <p>Enables MAC address spoof prevention for the specified VM group. Default setting is disabled.</p> <ul style="list-style-type: none"> o basic validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for “trusted” hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines. o advanced validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for “untrusted” hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines. <p>Command mode: Global configuration</p>
<p>no virt vmgroup <1-4096> validate</p> <p>Disables MAC address spoof prevention for the specified VM group.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> vm [<MAC address> <UUID> <name> <IP address> <index number>]</p> <p>Adds or removes a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (virt vmware vcspec). The VM index number is found in the VM information dump (show virt vm).</p> <p>Note: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> vmap <VMAP number> {intports extports}</p> <p>Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group.</p> <p>For more information about configuring VLAN Maps, see “VMAP Configuration” on page 266.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmgroup <1-4096> vport <virtual port alias or number></p> <p>Adds or removes the selected virtual port to the VM group.</p> <p>Command mode: Global configuration</p>

Table 216. *VM Group Commands (continued)*

Command Syntax and Usage
<p>virt vmgroup <1-4096> vlan <VLAN number></p> <p>Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group.</p> <p>Note: If you add a VM profile to this group, the group will use the VLAN assigned to the profile.</p> <p>Command mode: Global configuration</p>
<p>no virt vmgroup <1-4096></p> <p>Deletes the VM group.</p> <p>Command mode: Global configuration</p>
<p>show virt vmgroup <1-4096></p> <p>Displays the current VM group parameters.</p> <p>Command mode: All</p>

VM Check Configuration

Table 217 describes the VM Check validation options used for MAC address spoof prevention.

Table 217. *VM Check Configuration Options*

Command Syntax and Usage
<p>virt vmcheck acls max <1-256></p> <p>Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode.</p> <p>The default value is 50.</p> <p>Command mode: Global configuration</p>
<p>no virt vmcheck acls</p> <p>Disables ACL-based MAC address spoofing prevention in advanced validation mode.</p> <p>Command mode: Global configuration</p>
<p>virt vmcheck action advanced {acl link log}</p> <p>Sets up action taken when detecting MAC address spoofing in advanced validation mode:</p> <ul style="list-style-type: none"> o acl registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address o link registers a syslog entry and disables the corresponding switch port o log registers a syslog entry <p>The default setting is acl.</p> <p>Command mode: Global configuration</p>
<p>virt vmcheck action basic {link log}</p> <p>Sets up action taken when detecting MAC address spoofing in basic validation mode:</p> <ul style="list-style-type: none"> o link registers a syslog entry and disables the corresponding switch port o log registers a syslog entry <p>The default setting is link.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmcheck trust <ports></p> <p>Enables or disables trusted ports for VM communication.</p> <p>By default, all ports are disabled.</p> <p>Command mode: Global configuration</p>
<p>show virt vmcheck</p> <p>Displays the current VM Check settings. See page 92 for sample output.</p> <p>Command mode: Global configuration</p>

VM Profile Configuration

Table 218 describes the VM Profiles configuration options.

Table 218. VM Profiles Commands

Command Syntax and Usage
<p>virt vmprofile <profile name (1-39 characters)> Defines a name for the VM profile. Command mode: Global configuration</p>
<p>no virt vmprofile <profile name (1-39 characters)> Deletes the selected VM profile. Command mode: Global configuration</p>
<p>[no] virt vmprofile edit <profile name (1-39 characters)> eshaping [<i><average (1-1000000000)></i> <i><burst (1-1000000000)></i> <i><peak (1-1000000000)></i>] Configures traffic egress shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> o Average traffic, in Kilobits per second o Maximum burst size, in Kilobytes o Peak traffic, in Kilobits per second o Delete traffic shaping parameters. <p>Command mode: Global configuration</p>
<p>[no] virt vmprofile edit <profile name (1-39 characters)> shaping [<i><average (1-1000000000)></i> <i><burst (1-1000000000)></i> <i><peak (1-1000000000)></i>] Configures traffic shaping parameters implemented in the hypervisor, as follows:</p> <ul style="list-style-type: none"> o Average traffic, in Kilobits per second o Maximum burst size, in Kilobytes o Peak traffic, in Kilobits per second o Delete traffic shaping parameters. <p>Command mode: Global configuration</p>
<p>virt vmprofile edit <profile name (1-39 characters)> vlan <VLAN number> Assigns a VLAN to the VM profile. Command mode: Global configuration</p>
<p>show virt vmprofile [<i><profile name></i>] Displays the current VM Profile parameters. Command mode: All</p>

VMWare Configuration

Table 219 describes the VMware configuration options. When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

Note: VM Profiles and Hello cannot be configured or enabled unless the Virtual Center is configured.

Table 219. VM Ware Commands

Command Syntax and Usage
<p>virt vmware hbport <1-65535></p> <p>Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center.</p> <p>The default value is port 902.</p> <p>Command mode: Global configuration</p>
<p>virt vmware hello [enable haddr <IP_address> hport <port_no> htimer <1-60>]</p> <p>Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention.</p> <p>Default setting is disabled.</p> <ul style="list-style-type: none"> o enable enables CDP advertisements transmission. o haddr advertises a specific IP address instead of the default management IP. o hport enables ports on which CDP advertisements are sent. o htimer sets the number of seconds between successive CDP advertisements. Default value is 30. <p>Command mode: Global configuration</p>
<p>no virt vmware hello [enable hport <port_no>]</p> <p>Disables CDP advertisement transmissions completely or only on specific ports.</p> <p>Command mode: Global configuration</p>
<p>[no] virt vmware vcspec <IP address> <username> [noauth]</p> <p>Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system. You are prompted for the following information:</p> <ul style="list-style-type: none"> – IP address of the Virtual Center – User name and password for the Virtual Center – Whether to authenticate the SSL security certificate (yes or no) <p>Command mode: Global configuration</p>

Table 219. *VM Ware Commands*

Command Syntax and Usage
show virt vmware Displays the current VMware parameters. Command mode: All

Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the Lenovo N/OS CLI, ISCLI and the Miscellaneous VMready Configuration Menu. [Table 219](#) describes the VMready configuration options.

Table 220. *VMware Miscellaneous Options*

Command Syntax and Usage
[no] virt vmrmisc lmac Enables or disables the switch to treat locally administered MAC addresses as VMs. Command mode: Global configuration
[no] virt vmrmisc oui <3 byte VM MAC OUI> <Vendor Name> Adds or removes a MAC OUI. Command mode: Global configuration
show virt oui Displays all the configured MAC OUIs. Command mode: All

UFP Configuration

Table 221 describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 8 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, FCoE, auto) and within predefined bandwidth limits.

Note:

Table 221. *UFP Commands*

Command Syntax and Usage
<p>[no] ufp enable Globally enables or disables UFP. Command mode: Global configuration</p>
<p>[no] ufp port <port_no.> enable Enables or disables UFP on the specified physical ports. Command mode: Global configuration</p>
<p>[no] ufp port <port_no.> qos-mode [bw ets] Sets the UFP QoS mode: bandwidth or ETS. Command mode: Global configuration</p>
<p>ufp port <port_no.> vport <1-8> Enters UFP Virtual Port Configuration mode. Command mode: Global configuration</p>
<p>no ufp port <port_no.> [vport <1-8>] Disables UFP settings on the specified physical or virtual port. Command mode: Global configuration</p>
<p>[no] enable Enables or disables the virtual port. Command mode: UFP Virtual Port Configuration</p>
<p>evb profile <1-16> Applies the specified EVB profile for the virtual port. Command mode: UFP Virtual Port Configuration</p>
<p>no evb profile Disables the specified EVB profile for the virtual port. Command mode: UFP Virtual Port Configuration</p>

Table 221. UFP Commands (continued)

Command Syntax and Usage
<p>network {default-tag default-vlan <2-4094>}</p> <p>Configures the virtual port network configuration settings:</p> <ul style="list-style-type: none">o default-tag enables tagging egress frames with the default VLAN ID when the virtual port is in access or trunk mode and default-vlan is defined. Default setting is disabled.o default-vlan configures the default VLAN ID for the virtual port. <p>Note: VLANs 4002-4009 cannot be used as customer VLANs.</p> <p>Note: A customer VLAN cannot be configured on multiple virtual ports of the same physical port.</p> <p>Command mode: UFP Virtual Port Configuration</p>
<p>no network default-tag</p> <p>Disables default VLAN ID tagging on the virtual port.</p> <p>Command mode: UFP Virtual Port Configuration</p>
<p>network mode {access auto fcoe trunk tunnel}</p> <p>Configures the virtual port's operating mode:</p> <ul style="list-style-type: none">o access allows the virtual port to associate only with the default customer VLAN, as defined by the network default-vlan command.o auto integrates UFP with VMReady/802.1qbg. This mode allows dynamic vlan creation for the vport.o fcoe configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. Setting a virtual port in fcoe mode enables Priority Flow Control on the physical port.o trunk allows the virtual port to associate with up to 1024 customer VLANs.o tunnel makes the virtual port VLAN agnostic. This is the default setting. <p>Command mode: UFP Virtual Port Configuration</p>
<p>network private-vlan {host trunk promiscuous}</p> <p>Configures the virtual port's private VLAN mode:</p> <ul style="list-style-type: none">o host allows only ONE secondary VLAN. In case of network trunk mode, the other VLANs will be in different Private VLAN domain.o trunk allows both primary and secondary VLAN as well as non-Private VLAN domains. The Isolate-VLAN is also allowed to pass through this port type.o promiscuous allows private VLAN promiscuous mode <p>Command mode: UFP Virtual Port Configuration</p>

Table 221. *UFP Commands (continued)*

Command Syntax and Usage
<p>no network private-vlan</p> <p>Disables private-VLAN mode on the virtual port.</p> <p>Command mode: UFP Virtual Port Configuration</p>
<p>qos bandwidth {max <10-100> min <10-100>}</p> <p>Configures bandwidth allocation for the virtual port:</p> <ul style="list-style-type: none">o Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is 25.o Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is 100. <p>Note: The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100.</p> <p>Command mode: UFP Virtual Port Configuration</p>

Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). [Table 222](#) describes the EVB configuration options.

Table 222. *Edge Virtual Bridge Configuration Options*

Command Syntax and Usage
virt evb vsidb <VSIDB_number> Enter Virtual Station Interface Database configuration mode. Command mode: Global configuration
filename <file name> Sets the Virtual Station Interface Type database document name. Command mode: VSI Database
no filename Removes the Virtual Station Interface Type database document name. Command mode: VSI Database
filepath <file path> Sets the Virtual Station Interface Type database document path. Command mode: VSI Database
no filepath Removes the Virtual Station Interface Type database document path. Command mode: VSI Database
host <IP address> [mgt-port extm-port] Sets the Virtual Station Interface Type database manager IPv4/IPv6 address and the port used for the connection. By default, the management port is used. Command mode: VSI Database
port <1-65534> Sets the Virtual Station Interface Type database manager port. Command mode: VSI Database
protocol { http https } Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP. Command mode: VSI Database
update-interval <5-300> Sets the Virtual Station Interface Type database update interval in seconds. Command mode: VSI Database

Table 222. Edge Virtual Bridge Configuration Options

Command Syntax and Usage
no update-interval <5-300> Disables periodic updates. Command mode: VSI Database
no virt evb vsidb <VSIDB_number> Resets the Virtual Station Interface Type database information to the default values. Command mode: Global configuration
clear virt evb vsi [mac-address port <port alias or number> type-id <1-16777215> vlan <1-4094>] Clears VSI database associations. Command mode: All
clear virt evb vsidb [manager-id <0-255> type-id <1-16777215> version <0-255>] Clears local VSI types cache. Command mode: All
show virt evb vsitypes [mgrid <0-255> typeid <1-16777215> version <0-255>] Displays the current Virtual Station Interface Type database parameters. Command mode: All
show virt evb vsidb <VSIDB_number> Displays the current Virtual Station Interface database information. Command mode: All

Edge Virtual Bridge Profile Configuration

Table 223 describes the Edge Virtual Bridge profile configuration options.

Table 223. *Edge Virtual Bridge VSI Type Profile Configuration Options*

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

Switch Partition (SPAR) Configuration

Switch partitions (SPARs) divide the data plane inside a physical switch into independent switching domains. Switch partitions do not communicate with each other, forcing hosts on different SPARs to bridge traffic over an upstream link, even if they belong to the same VLAN.

Up to 8 SPARs can be defined on a switch. Each SPAR supports up to 256 local VLANs, for further partitioning flexibility.

Table 224. *SPAR Configuration Options*

Command Syntax and Usage
spar <1-8> Enters SPAR Configuration mode. Command mode: Global configuration
no spar <1-8> Deletes the specified SPAR. Command mode: Global configuration
[no] enable Enables or disables the SPAR. Command mode: SPAR Configuration
name Configures the SPAR name. Command mode: SPAR Configuration
domain default {vlan <2-4094> member <port no.>} Configures the SPAR's default domain settings: <ul style="list-style-type: none">o vlan configures the default SPAR VLAN ID. A unique factory default VLAN ID is assigned to each SPAR as "408x", where x is the SPAR ID <1-8>. This option provides an override if conflicts arise with a customer VLAN ID on the upstream network.o member adds server ports to the SPAR. Command mode: SPAR Configuration
no domain default member <port no.> Removes server ports from the SPAR. Command mode: SPAR Configuration

Table 224. SPAR Configuration Options (continued)

<p>Command Syntax and Usage</p>
<p>domain local <1-256> {enable member <port no.> name <text> vlan <2-4094>}</p> <p>Configures the SPAR's local domains:</p> <ul style="list-style-type: none"> o enable enables the SPAR local domains o member adds server ports to the SPAR local domains o name configures the SPAR local domains names o vlan applies a VLAN ID to the SPAR local domains. The default value is 0. <p>Command mode: SPAR Configuration</p>
<p>no domain local <1-256> [enable member <port no.> vlan]</p> <p>Deletes the SPAR local VLAN domains:</p> <ul style="list-style-type: none"> o enable disables the SPAR local domains o member deletes SPAR local domains server ports o vlan deletes SPAR local domains vlan. <p>Command mode: SPAR Configuration</p>
<p>domain mode {passthrough local}</p> <p>Configures the SPAR domain mode:</p> <ul style="list-style-type: none"> o passthrough references member ports only by the SPAR default VLAN. This provides VLAN-unaware uplink connectivity via pass-through tunnel domain switching for SPAR member ports. The default value is passthrough. o local references member ports by both SPAR default VLAN and SPAR local domain VLANs. This provides VLAN-aware uplink connectivity via local domain switching for SPAR member ports <p>Command mode: SPAR Configuration</p>
<p>[no] uplink {port <port no.> portchannel <1-64> adminkey <1-65535>}</p> <p>Enables or disables uplink connectivity for the SPAR. A single external port, portchannel, or LACP channel can be used for uplink. All uplinks within a SPAR are automatically assigned to the SPAR domain's default VLAN and to any SPAR local VLANs.</p> <p>Command mode: SPAR Configuration</p>
<p>show spar <1-8> [domain [default local <1-256>] uplink]</p> <p>Displays the SPAR settings:</p> <ul style="list-style-type: none"> o domain filters only the SPAR domain related settings <ul style="list-style-type: none"> • default filters only SPAR default domain settings • local <1-256> filters only SPAR local domains settings o uplink filters only SPAR uplink settings <p>Command mode: All</p>

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 SI4093 System Interconnect Module behaves as a Service Agent providing systems management services.

Table 225. *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 4093(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on [page 354](#).

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 4093(config)# copy running-config ftp [extm-port|mgt-port]
```

or:

```
SI 4093(config)# copy running-config tftp [extm-port|mgt-port]
```

or:

```
SI 4093(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 4093(config)# copy ftp running-config [extm-port|mgt-port]
```

or:

```
SI 4093(config)# copy tftp running-config [extm-port|mgt-port]
```

or:

```
SI 4093(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 226. *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 227. *Port Operations Commands*

Command Syntax and Usage
<p>no interface port <port number or alias> shutdown</p> <p>Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p>Command Mode: Privileged EXEC</p>
<p>interface port <port number or alias> shutdown</p> <p>Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.</p> <p>Command Mode: Privileged EXEC</p>
<p>[no] interface portchannel <1-128> shutdown</p> <p>Temporarily enables or disables the specified port channel. The port channel will be returned to its configured operation mode when the switch is reset.</p> <p>Command Mode: Privileged EXEC</p>
<p>[no] interface portchannel lacp <1-65535> shutdown</p> <p>Temporarily enables or disables specified LACP trunk groups.</p> <p>Command Mode: Privileged EXEC</p>
<p>show interface port <port number or alias> operation</p> <p>Displays the port interface operational state.</p> <p>Command Mode: Privileged EXEC</p>

Protected Mode Options

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

Table 228. *Protected Mode Options*

Command Syntax and Usage
<p>[no] protected-mode enable</p> <p>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.</p> <p>Command Mode: Global Configuration</p>
<p>[no] protected-mode external-management</p> <p>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.</p> <p>The default value is enabled.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<p>[no] protected-mode external-ports</p> <p>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.</p> <p>The default value is enabled.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<p>[no] protected-mode factory-default</p> <p>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.</p> <p>The default value is enabled.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>

Table 228. *Protected Mode Options (continued)*

Command Syntax and Usage
<p>[no] protected-mode management-vlan-interface</p> <p>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.</p> <p>The default value is enabled.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<p>show protected-mode</p> <p>Displays the current Protected Mode configuration.</p> <p>Command Mode: Global Configuration</p>

VMware Operations

Use these commands to perform minor adjustments to the VMware operation. Use these commands to perform Virtual Switch operations directly from the switch. Note that these commands require the configuration of Virtual Center access information (**virt vmware vcspec**).

Table 229. *VMware Operations Commands*

Command Syntax and Usage
<p>virt vmware pg [<i><Port Group name></i> <i><host ID></i> <i><VSwitch name></i> <i><VLAN number></i> <i><shaping-enabled></i> <i><average-Kbps></i> <i><burst-KB></i> <i><peak-Kbps></i>]</p> <p>Adds a Port Group to a VMware host. You are prompted for the following information:</p> <ul style="list-style-type: none"> o Port Group name o VMware host ID (Use host UUID, host IP address, or host name.) o Virtual Switch name o VLAN ID of the Port Group o Whether to enable the traffic-shaping profile (1 or 0). If you choose 1 (yes), you are prompted to enter the traffic shaping parameters. <p>Command Mode: All</p>
<p>no virt vmware pg <i><Port Group name></i> <i><host ID></i></p> <p>Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> o UUID o IP address o Host name <p>Command Mode: All</p>
<p>[no] virt vmware vsw <i><host ID></i> <i><Virtual Switch name></i></p> <p>Adds or removes a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> o UUID o IP address o Host name <p>Command Mode: All</p>

Table 229. *VMware Operations Commands (continued)*

Command Syntax and Usage
<p>virt vmware export <VM profile name> <VMware host ID> <Virtual Switch name></p> <p>Exports a VM Profile to a VMware host.</p> <p>Use one of the following identifiers to specify each host:</p> <ul style="list-style-type: none">o UUIDo IP addresso Host name <p>You may enter a Virtual Switch name, or enter a new name to create a new Virtual Switch.</p> <p>Command Mode: All</p>
<p>virt vmware scan</p> <p>Performs a scan of the VM Agent, and updates VM information.</p> <p>Command Mode: All</p>
<p>virt vmware vmacpg <MAC address> <Port Group name></p> <p>Changes a VM NIC's configured Port Group.</p> <p>Command Mode: All</p>
<p>virt vmware updp <Port Group name> <host ID> <VLAN number> [<shaping enabled> <average Kbps> <burst KB> <peak Kbps>]</p> <p>Updates a VMware host's Port Group parameters.</p> <p>Command Mode: All</p>

VMware Distributed Virtual Switch Operations

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

Table 230. VMware dvSwitch Operations (*/oper/virt/vmware/dvswitch*)

Command Syntax and Usage
<p>virt vmware dvswitch add <datacenter name> <dvSwitch name> <dvSwitch version></p> <p>Adds the specified dvSwitch to the specified DataCenter.</p> <p>Command Mode: All</p>
<p>virt vmware dvswitch del <datacenter name> <dvSwitch name></p> <p>Removes the specified dvSwitch from the specified DataCenter.</p> <p>Command Mode: All</p>
<p>virt vmware dvswitch addhost <dvSwitch name> {<host UUID IP address host name>}</p> <p>Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> o UUID o IP address o Host name <p>Command Mode: All</p>
<p>virt vmware dvswitch remhost <dvSwitch name> {<host UUID IP address host name>}</p> <p>Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host:</p> <ul style="list-style-type: none"> o UUID o IP address o Host name <p>Command Mode: All</p>
<p>virt vmware dvswitch addUplink <dvSwitch name> <host ID> <uplink name></p> <p>Adds the specified physical NIC to the specified dvSwitch uplink ports.</p> <p>Command Mode: All</p>
<p>virt vmware dvswitch remUplink <dvSwitch name> <host ID> <uplink name></p> <p>Removes the specified physical NIC from the specified dvSwitch uplink ports.</p> <p>Command Mode: All</p>

VMware Distributed Port Group Operations

Use these commands to administer a VMware distributed port group.

Table 231. VMware Distributed Port Group Operations (*/oper/virt/vmware/dpg*)

<p>Command Syntax and Usage</p> <p>virt vmware dpg add <port group name> <dvSwitch name> <VLAN ID> [ishaping <bandwidth> <burst size> <peak bandwidth>] [eshaping <bandwidth> <burst size> <peak bandwidth>]</p> <p>Adds the specified port group to the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> o ishaping: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second o eshaping: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second <p>Command Mode: All</p>
<p>virt vmware dpg vmac <VNIC MAC> <port group name></p> <p>Adds the specified VM NIC to the specified port group.</p> <p>Command Mode: All</p>
<p>virt vmware dpg update <port group name> <dvSwitch name> <VLAN ID> [ishaping <bandwidth> <burst size> <peak bandwidth>] [eshaping <bandwidth> <burst size> <peak bandwidth>]</p> <p>Updates the specified port group on the specified dvSwitch. You may enter the following parameters:</p> <ul style="list-style-type: none"> o ishaping: Enables ingress shaping. Supply the following information: <ul style="list-style-type: none"> • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second o eshaping: Enables egress shaping. Supply the following information: <ul style="list-style-type: none"> • average bandwidth in KB per second • burst size in KB • peak bandwidth in KB per second <p>Command Mode: All</p>
<p>virt vmware dpg del <port group name> <dvSwitch name></p> <p>Removes the specified port group from the specified dvSwitch.</p> <p>Command Mode: All</p>

Edge Virtual Bridge Operations

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

Table 232. *Edge Virtual Bridge Operations Commands*

Command Syntax and Usage
virt evb update vsidb <VSIDB_number> Update VSI types from the VSI database. Command mode: All
clear virt evb vsidb [mgrid <0-255> typeid <1-16777215> version <0-255>] Clears local VSI types cache. Command mode: Privileged EXEC
clear virt evb vsi [mac-address port <port alias or number> type-id <1-16777215> vlan <1-4094>] Clears VSI database associations. Command mode: Privileged EXEC

Feature on Demand Key Options

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

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

show interface information

Table 233. *Feature on Demand Key Options*

Command Syntax and Usage
<p>software-key</p> <p>Enter FOD Key mode.</p> <p>Command mode: Privileged EXEC</p>
<p>enakey address <i><hostname or IP address></i> keyfile <i><file name></i> protocol {tftp sftp} mgt</p> <p>Unlocks the software port expansion feature. You are prompted to enter the host name or IP address of the server where the license key is stored, and the license key file name, as follows:</p> <ul style="list-style-type: none"> o 46Port o 64Port <p>Note: You must upgrade to 46Port port mode before you can upgrade to 64Port port mode.</p> <p>Command mode: FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p>copy tftp software-key address <i><hostname or IP address></i> keyfile <i><file name></i> mgt</p>
<p>ptkey address <i><hostname or IP address></i> key <i><feature name></i> protocol {tftp sftp} file <i><file name></i> mgt</p> <p>Loads the specified key file to a server.</p> <p>Command mode: FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p>copy software-key address <i><hostname or IP address></i> key <i><file name></i> protocol {tftp sftp} file <i><file name></i> mgt</p>

Table 233. *Feature on Demand Key Options*

Command Syntax and Usage
<p>invkeys address <i><hostname or IP address></i> invfile <i><file name></i> protocol {tftp sftp} mgt</p> <p>Loads key code inventory information to a server.</p> <p>Command mode: FOD Key mode</p> <p>Use the following command to perform the same action, regardless the command mode:</p> <p>copy invkeys address <i><hostname or IP address></i> invfile <i><file name></i> protocol {tftp sftp} mgt</p>
<p>rmkey key <i><feature name></i></p> <p>Removes the specified software feature.</p> <p>Command mode: FOD Key mode</p>
<p>exit</p> <p>Exit from Feature on Demand Key mode.</p> <p>Command mode: FOD Key mode</p>
<p>show software-key</p> <p>Shows software licensing keys.</p> <p>Command mode: All</p>

Chapter 6. Boot Options

To use the Boot Options commands, you must be logged in to the switch as the administrator. The Boot Options commands provide options for:

- Selecting a switch software image to be used when the switch is next reset
- Selecting a configuration block to be used when the switch is next reset
- Downloading or uploading a new software image to the switch via FTP/TFTP

In addition to the Boot commands, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Working with Switch Images and Configuration Files” in the *Command Reference*.

The boot options are discussed in the following sections.

Scheduled Reboot

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

Table 234. *Boot Scheduling Options*

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

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 235. *Netboot Options (/boot/netboot)*

Command Syntax and Usage
<p>[no] boot netboot enable</p> <p>Enables or disables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.</p> <p>Command mode: Global configuration</p>
<p>[no] boot netboot tftp <IP address></p> <p>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.</p> <p>Command mode: Global configuration</p>
<p>[no] boot netboot cfgfile <1-31 characters></p> <p>Defines the file path for the configuration file on the TFTP server. For example: /directory/sub/config.cfg</p> <p>Command mode: Global configuration</p>
<p>show boot</p> <p>Displays the current Netboot parameters.</p> <p>Command mode: All</p>

Flexible Port Mapping

Depending on the license keys installed on the switch, only a limited number of physical ports might be active. Flexible Port Mapping allows you to alter the default configuration set up by the license, by manually setting up which ports are active or inactive.

Active ports may not collectively exceed the bandwidth limit imposed by the current license level.

[Table 236](#) lists the Flexible Port Mapping command options.

Table 236. *Flexible Port Mapping Options*

Command Syntax and Usage
[no] boot port-map <i><port number or range></i> Enables or disables the specified ports. Command mode: Global configuration
default boot port-map Reverts the port mapping to the default licensed configuration. Command mode: Global configuration
show boot port-map Displays the total bandwidth available, current port mapping and configured port mapping. Command mode: All

QSFP Port Configuration

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

Table 237. *Netboot Options (/boot/qsfp-40Gports)*

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

Updating the Switch Software Image

The switch software image is the executable code running on the SI4093 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 4093# copy {ftp|tftp|sftp} {image1|image2|boot-image} [extm-port | mgt-port | data-port]
```

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

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

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

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

The exact form of the name will vary by server. However, the file location is normally relative to the FTP, SFTP or TFTP directory (usually `tftpboot`).

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

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

5. The system prompts you to confirm your request.

Next, select a software image to run, as described in the following section.

Selecting a Software Image to Run

You can select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.

1. In Global Configuration mode, enter:

```
SI 4093(config)# boot image {image1|image2}
```

2. Enter the name of the image you want the switch to use upon the next boot.

The system informs you of which image set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

Uploading a Software Image from Your Switch

You can upload a software image from the switch to a FTP, SFTP or TFTP server.

1. In Privileged EXEC mode, enter:

```
SI 4093# copy {image1|image2|boot-image} {ftp|tftp|sftp}  
[extm-port|mgt-port|data-port]
```

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

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

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

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

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

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

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

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

```
image2 currently contains Software Version 6.5.0  
that was downloaded at 0:23:39 Thu Jan 1, 2010  
Upload will transfer image2 (2788535 bytes) to file "image1"  
on FTP/TFTP server 1.90.90.95.  
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the SI4093 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 SI4093 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 SI4093 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 4093(config)# boot configuration-block {active|backup|factory}
```

Rebooting the Switch

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

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

```
SI 4093# 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 378](#).
- 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 379](#).
- 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 381](#).
- To enable the loading of an unofficial image, press P and follow the screen prompts. For more details, see [“Physical Presence” on page 383](#).
- 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: SI4093-8.2.1.0_OS.img
    Netmask : 255.255.255.128
    Gateway : 10.241.6.66
Configuring management port.....
Installing image SI4093-8.2.1.0_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 SI4093-8.2.1.0_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:
 - o Speed: 9600 bps
 - o Data Bits: 8
 - o Stop Bits: 1
 - o Parity: None
 - o 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 379](#))
- XModem Download (for details, see [page 381](#))

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 SI4093 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 238. *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 396 . 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 396 . 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 396 . 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 238. *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 SI4093 information, statistics, and configuration. You can log the output (tsdmp) into a file. To filter the information, use the following options: <ul style="list-style-type: none">o l2 displays only Layer 2-related informationo l3 displays only Layer 3-related informationo link displays only link status-related informationo 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 239. *FDB Manipulation Commands*

Command Syntax and Usage
<p>show mac-address-table address <MAC address></p> <p>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:</p> <ul style="list-style-type: none">o xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56)o xxxxxxxxxxxxxx (such as 080020123456) <p>Command mode: All</p>
<p>show mac-address-table configured-static</p> <p>Displays configured static entries in the FDB.</p> <p>Command mode: All</p>
<p>show mac-address-table interface port <port number or alias></p> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All</p>
<p>show mac-address-table multicast</p> <p>Displays all Multicast MAC entries in the FDB.</p> <p>Command mode: All</p>
<p>show mac-address-table portchannel <LAG number></p> <p>Displays all FDB entries for a particular LAG.</p> <p>Command mode: All</p>
<p>show mac-address-table private-vlan <VLAN number></p> <p>Displays all FDB entries on a single private VLAN.</p> <p>Command mode: All</p>
<p>show mac-address-table state {forward trunk unknown}</p> <p>Displays all FDB entries of a particular state.</p> <p>Command mode: All</p>
<p>show mac-address-table static</p> <p>Displays static entries in the FDB.</p> <p>Command mode: All</p>

Table 239. 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 240. *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 240. *Miscellaneous Debug Commands*

Command Syntax and Usage
<p>[no] debug lACP packet {receive transmit both} port <i><port alias or numbers></i></p> <p>Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on specific ports running LACP.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none">o receive filters only LACP packets receivedo transmit filters only LACP packets sento both filters LACP packets either sent or received <p>By default, LACP debugging is disabled.</p> <p>Command mode: All except User EXEC</p>
<p>[no] debug ssh client {all state}</p> <p>Enables or disables SSH client based debug messages.</p> <ul style="list-style-type: none">o all: Enables or disables all SSH client debug messageso state: Enables or disables SSH client state debug messages <p>Command mode: All except User EXEC</p>
<p>[no] debug ssh server {all disconnect msg packet state}</p> <p>Enables or disables SSH server based debug messages.</p> <ul style="list-style-type: none">o all: Enables or disables all SSH server debug messages.o disconnect: Enables or disables SSH server disconnect debug messageso msg: Enables or disables SSH server type and protocol debug messageso packet: Enables or disables SSH server type, protocol and packet debug messageso state: Enables or disables SSH server state debug messages <p>Command mode: All except User EXEC</p>
<p>[no] debug tacacs-client</p> <p>Enables or disables TACACS+ client based debug messages.</p> <p>Command mode: All except User EXEC</p>
<p>clear flash-config</p> <p>Deletes all flash configuration blocks.</p> <p>Command mode: All except User EXEC</p>

LLDP Cache Manipulation

Table 241 describes the LLDP cache manipulation commands.

Table 241. *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 242 describes the IGMP group maintenance commands.

Table 242. 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 243. *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 244](#) describes the IPv6 Neighbor Discovery cache manipulation commands.

Table 244. *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 <i><IPv6 address></i> Shows a single IPv6 Neighbor Discovery cache entry by IP address. Command mode: All
show ipv6 neighbors interface port <i><port number or alias></i> 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 <i><VLAN number></i> 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 245 describes the IPv6 route maintenance commands.

Table 245. *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 ftp`), 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 4093# 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 4093# 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 4093# 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 4093# clear flash-dump
```

The switch clears the dump region of flash memory and displays the following message:

```
FLASH dump region cleared.
```

If the flash dump region is already clear, the switch displays the following message:

```
FLASH dump region is already clear.
```

Appendix A. Lenovo N/OS System Log Messages

The SI4093 System Interconnect Module (SI4093) 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>
VRRP	Received <x> virtual routers instead of <y>
VRRP	received errored advertisement from <IP address>
VRRP	received incorrect addresses from <IP address>
VRRP	received incorrect advertisement interval <interval> from <IP address>
VRRP	received incorrect VRRP authentication type from <IP address>
VRRP	received incorrect VRRP password from <IP address>
VRRP	VRRP : received incorrect IP addresses list from <IP address>

LOG_CRIT

Thread	LOG_CRIT Message
AUDIT	NTP: cannot contact NTP server %s
AUDIT	NTP: System clock not updated. Authentication failed
AUDIT	VRRP: received incorrect VRRP authentication from %s
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private public key}
SYSTEM	System memory is at <n> percent

LOG_ERR

Thread	LOG_ERR Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP {Copy cfgRcv} attempting to redirect a previously redirected output
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX APP advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX APP willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PFC advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PFC willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PG advertise settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX PG willing settings.
DCBX	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different DCBX state settings.
MGMT	Apply is issued by another user. Try later
MGMT	Critical Error. Failed to add Interface <interface>
MGMT	Diff is issued by another user. Try later
MGMT	Dump is issued by another user. Try later
MGMT	Error: Apply not done
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory)
MGMT	Revert Apply is issued by another user. Try later
MGMT	Revert is issued by another user. Try later.
MGMT	Save is issued by another user. Try later

Thread	LOG_ERR Message (continued)
NTP	unable to listen to NTP port
PFC	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different PFC settings.
PFC	Ports <port alias or number> and <port alias or number> in trunk group <trunk number> have different PFC settings for priority <priority number>.
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Not enough memory!

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user <username>.
	System log cleared via SNMP.
AUDIT	Audit log has been cleared by %s
AUDIT	Class of service for user %s is changed
AUDIT	HTTPS has been disabled
AUDIT	HTTPS has been enabled
AUDIT	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> ejected from BBI
MGMT	<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	<username>(<user type>) login {on Console from host <IP address>}
MGMT	boot kernel download completed. Now writing to flash.

Thread	LOG_INFO Message (continued)
MGMT	boot kernel downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image image1 image2 boot kernel undefined SP boot kernel}
MGMT	Firmware downloaded to {invalid image image1 image2 boot kernel undefined SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <hostname>:<filename>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1 2 download completed. Now writing to flash.
MGMT	image1 2 downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	image1 2 downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
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

Thread	LOG_INFO Message (continued)
MGMT	new configuration applied [from BBI EM SCP SNMP]
MGMT	new configuration saved from {BBI ISCLI SNMP}
MGMT	scp <username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	scp <username>(<user type>) login {on Console from host <IP address>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	SP boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Starting Firmware download for {invalid image image1 image2 boot kernel undefined SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <hostname>:<filename>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	undefined downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	unsaved changes reverted [from BBI from SNMP]
MGMT	Unsupported GBIC {accepted refused}
MGMT	user {SNMP user <username>} ejected from BBI
MGMT	Watchdog has been {enabled disabled}
MGMT	Watchdog timeout interval is now <seconds> seconds)
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

Thread	LOG_INFO 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	server key autogen {starts completes}
SSH	Wrong config file type
SYSTEM	booted version <version> from Flash image <image>, {active backup factory} config block

LOG_NOTICE

Thread	LOG_NOTICE Message
	Current config successfully tftp'd <filename> from <hostname>
	Current config successfully tftp'd to <hostname>: <filename>
	Port <port> mode is changed to full duplex for 1000 Mbps operation.
AUDIT	DHCP: Offer was found invalid by ip configuration
CONSOLE	RADIUS: authentication timeout. Retrying...
CONSOLE	RADIUS: failed to contact primary secondary server
CONSOLE	RADIUS: No configured RADIUS server
CONSOLE	RADIUS: trying alternate server...
HOTLINKS	"Error" is set to "Standby Active"
HOTLINKS	"Learning" is set to "Standby Active"
HOTLINKS	"None" is set to "Standby Active"
HOTLINKS	"Side Max" is set to "Standby Active"
HOTLINKS	has no "{Side Max None Learning Error}" interface
MGMT	<username> automatically logged out from BBI because changing of authentication type
MGMT	<username>(<user type>) {logout ejected idle timeout connection closed} from {BBI Console Telnet/SSH}
MGMT	<username>(<user type>) login {on Console from host <IP address> from BBI}
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Password incorrect!
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	enable password changed
MGMT	Error in setting the new config
MGMT	Failed login attempt via {BBI TELNET} from host <IP address>.
MGMT	Failed login attempt via the CONSOLE

Thread	LOG_NOTICE Message (continued)
MGMT	FLASH Dump cleared from BBI
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper operator} changed by {SNMP user <username>}, notifying admin to save.
MGMT	QSFP: Port <port> changed to {10G 40G}, from {BBI SNMP CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp <username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	scp <username>(<user type>) login {on Console from host <IP address>}
MGMT	second syslog host changed to {this host <IP address>}
MGMT	selectable [boot] mode changed
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host <IP address>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Terminating BBI connection from host <IP address>
MGMT	User <username> deleted by {SNMP user <username>}.
MGMT	User <username> is {deleted disabled} and will be ejected by {SNMP user <username>}
MGMT	User {oper operator} is disabled and will be ejected by {SNMP user <username>}.
MGMT	Wrong config file type
NTP	System clock updated
SERVER	link {down up} on port <port>
SSH	(remote disconnect msg)

Thread	LOG_NOTICE Message (continued)
SSH	<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
SSH	<username>(<user type>) login {on Console from host <IP address>}
SSH	Error in setting the new config
SSH	Failed login attempt via SSH
SSH	New config set
SSH	scp <username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
SSH	scp <username>(<user type>) login {on Console from host <IP address>}
SSH	Wrong config file type
SYSTEM	Change fiber GIG port <port> mode to full duplex
SYSTEM	Change fiber GIG port <port> speed to 1000
SYSTEM	Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN>
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Port <port> disabled
SYSTEM	Port <port> disabled due to reason code <reason code>
SYSTEM	rebooted (<reason>)[, administrator logged in] Reason: <ul style="list-style-type: none"> ● Boot watchdog reset ● console PANIC command ● console RESET KEY ● hard reset by SNMP ● hard reset by WEB-UI ● hard reset from console ● hard reset from Telnet ● low memory ● MM Cycled Power Domain ● power cycle ● Reset Button was pushed ● reset by SNMP ● reset by WEB-UI ● reset from console ● reset from EM ● reset from Telnet/SSH ● scheduled reboot ● SMS-64 found an over-voltage ● SMS-64 found an under-voltage ● software ASSERT ● software PANIC ● software VERIFY ● Telnet PANIC command ● unknown reason ● watchdog timer
SYSTEM	Received BOOTP Offer: IP: <IP address>, Mask: <netmask>, Broadcast <IP address>, GW: <IP address>

Thread	LOG_NOTICE Message (continued)
SYSTEM	Watchdog threshold changed from <i><old value></i> to <i><new value></i> seconds
SYSTEM	Watchdog timer has been enabled
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
TEAMING	is down, control ports are auto disabled
TEAMING	is up, control ports are auto controlled
VLAN	Default VLAN can not be deleted
VRRP	virtual router <i><IP address></i> is now {BACKUP MASTER}
WEB	<i><username></i> ejected from BBI
WEB	RSA host key is being saved to Flash ROM, please don't reboot the box immediately.

LOG_WARNING

Thread	LOG_WARNING Message
AUDIT	DHCP: disable
AUDIT	DHCP: enable
AUDIT	DHCP: Enabling DHCP will overwrite IP interface %d and IP gateway %d's configurations.
AUDIT	DHCP: on External Management Interface disabled with I2C Control Register
AUDIT	DHCP: on External Management Interface enabled with I2C Control Register
AUDIT	DHCP: Use factory default while requesting for a new DHCP offer.
AUDIT	Failed login attempt via the %s
AUDIT	IP: ARP table is full.
AUDIT	IP: Changed ARP entry for IP %s to: \tMAC %02x:%02x:%02x:%02x:%02x:%02x
AUDIT	IP: gateway %s is down
AUDIT	IP: gateway %s is up
AUDIT	IP: New Management Gateway %s configured
AUDIT	IP: New Management IP Address %s configured
AUDIT	IP: Route table full
AUDIT	LDAP security does not meet security strict mode requirements
AUDIT	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.

Thread	LOG_WARNING Message (continued)
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
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	<ul style="list-style-type: none"> The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2¹. 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	<ul style="list-style-type: none"> Copper: Class G1 as per ANSI/ISA 71.04-1985³ 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.

 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 Betriebsmitteln

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 Paragraph 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

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

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

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

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

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

Japan VCCI Class A Statement

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

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

Japan Electronics and Information Technology Industries Association (JEITA) Statement

高調波ガイドライン適合品

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

高調波ガイドライン準用品

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

Korea Communications Commission (KCC) Statement

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

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

Russia Electromagnetic Interference (EMI) Class A Statement

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

People's Republic of China Class A electronic emission Statement

中华人民共和国“A类”警告声明

声明

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

Taiwan Class A compliance Statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
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

- 802.1p
 - and ETS 324
 - configuration 251, 273
 - DCBX PFC information 116
 - information 74, 75, 76, 119
 - PFC configuration 325
 - Priority Group mapping 119
 - priority level 238, 258, 266
 - IPv6 263
 - priority value 275

A

- abbreviating commands (CLI) 22
- access control
 - switch 231
 - user 233
- Access Control List (see ACL) 77
- ACL
 - add group 247
 - and VMAP 266
 - configuration 257
 - Ethernet matching criteria 259
 - filtering criteria 258
 - groups 257
 - information 77, 78
 - IPv4 matching criteria 260
 - IPv6 263
 - list of FIPS ACLs 121, 122
 - metering configuration 272
 - Packet Format matching criteria 262
 - port ACL configuration 247
 - port configuration commands 247
 - QoS parameters 247
 - re-marking 273
 - re-marking (IPv6) 275
 - remove group 247
 - statistics 181, 182
 - TCP matching criteria 261
 - UDP matching criteria 261
- active
 - configuration block 194, 375
 - switch configuration
 - ptcfg 353
 - restoring 354
 - saving and loading 354
- administrator account 23
- assistance, getting 415
- Australia Class A statement 424

B

- backup configuration block 375
- bandwidth allocation, Priority Groups 324
- boot
 - options 367 to ??
- Boot Management menu 377

C

- Canada Class A electronic emission statement 424
- CEE
 - configuration 323
 - information 111
- China Class A electronic emission statement 427
- Cisco Ether Channel 286
- Class A electronic emission notice 424
- clear
 - ACL statistics 181
 - all defined management networks 232
 - all IPv4 statistics 151, 154
 - all IPv6 statistics 151, 159
 - DNS statistics 151
 - dump information 397
 - FCoE statistics 183
 - Hot Links statistics 145
 - IGMP statistics 151
 - LACP statistics 145
 - statistics for specific ports 128, 145
 - statistics on a specific trunk group 144
 - TCP statistics 151
 - UDP statistics 151
- commands
 - abbreviations 22
 - conventions used in this manual 14
 - help with 20
 - shortcuts 22
 - tab completion 22

- configuration
 - commands 193 to 354
 - default gateway interval, for health checks 311
 - default gateway IP address 311
 - dump command 352
 - failover 295
 - flow control 244
 - IGMP 313
 - port link speed 244
 - port mirroring 277
 - port trunking 286
 - save changes 194
 - SNMP 217
 - switch IP address 307
 - TACACS+ 208
 - VLAN default (PVID) 240
 - VLAN tagging 239
 - VMware 341
- configuration block
 - active 375
 - backup 375
 - factory 375
 - selection 375
- contamination, particulate and gaseous 422
- Control Plane Protection, configuration 253
- Converged Enhanced Ethernet (see CEE) 111
- COPP, configuration 253
- COS queue information 75
- CPU use
 - history 180
 - statistics 178, 180

D

- daylight saving time 196
- DCB Capability Exchange Protocol (see DCBX) 112
- DCBX
 - Application Protocol information 117
 - configuration 327
 - control information 113
 - ETS information 115
 - feature information 114
 - information 112
 - PFC information 116
- debugging 385
- default gateway
 - information 60
 - interval, for health checks 311
 - IPv6 321
- default password 23

- delete
 - ACL statistics 181
 - all defined management networks 232
 - all IPv4 statistics 151, 154
 - all IPv6 statistics 151, 159
 - DNS statistics 151
 - dump information 397
 - Hot Links statistics 145
 - IGMP statistics 151
 - LACP statistics 145
 - statistics for specific ports 128, 145
 - statistics on a specific trunk group 144
 - TCP statistics 151
 - UDP statistics 151
- DHCP
 - and managed address configuration flag 309
 - and Netboot configuration 369
 - and other stateful configuration flag 309
- DiffServ Code Point (see DSCP) 252
- disconnect idle timeout 24
- downloading software 372
- DSCP
 - configuration 252
 - disable for in-profile traffic 274
 - re-mark for in-profile traffic 276
 - re-mark for out-profile traffic 276
 - re-marking configuration 238, 252
 - set value of in-profile packets 274
 - set value of out-profile packets 274
- dump
 - configuration command 352
 - maintenance 385
- duplex mode
 - interface status 25
 - link status 83

E

- ECN (Explicit Congestion Notification) 255
- Edge Virtual Bridging, configuration 346
- electronic emission Class A notice 424
- Enhanced Transmission Selection (see ETS) 119
- ENode 329
- Error Disable and Recovery
 - port 243
 - system 199
- EtherChannel, and port trunking 286
- ETS
 - configuration 324
 - information 112, 115, 119
 - Priority Group configuration 324
- European Union EMC Directive conformance statement 425
- EVB
 - configuration 346
 - configuration mode 19
 - information 98
- Explicit Congestion Notification (ECN) 255

F

- factory configuration block 375
- failover
 - auto monitor configuration 296
 - configuration 295
 - Layer 2 configuration 295
 - Layer 2 information 43, 49
 - manual monitor port configuration 297
 - trigger configuration 296
- FCC Class A notice 424
- FCC, Class A 424
- FCF port 329
- FCoE
 - configuration 328
 - FIPS port configuration 329
 - forwarding 329
 - information 121
 - Initialization Protocol (see FIP) 329
 - statistics 183
- FDB
 - configuration 279
 - configuring static entries 281
 - hot links update 299
 - information 44
 - learning 238
 - maintenance 385, 387
 - troubleshooting 385, 387
- Fiber Channel Initialization Protocol (see FIP) 121
- Fibre Channel over Ethernet (see FCoE) 121
- FIP
 - Snooping (see FIPS) 329
 - snooping information 121
- FIPS
 - list of ACLs 121
 - port configuration 329
- flow control
 - configuring 244
 - configuring for port link 244
 - information 25, 83
 - Ingress Back Pressure 135
 - pause packets 133, 134
 - priority (see PFC) 116
- Forwarding Database (see FDB) 44
- forwarding state (FWD) 45
- FWD (port state) 45

G

- gaseous contamination 422
- Germany Class A statement 425
- getting help 415
- gtcfcg (TFTP load command) 354

H

- health checks
 - default gateway interval, retries 311
 - retry, number of failed health checks 311
- help
 - online 20
 - sources of 415
- help, getting 415
- Hot Links configuration 299

I

- idle timeout, setting 24
- IEEE standards
 - 802.1p 251
- IGMP
 - advanced parameters 319
 - configuration 313
 - filter definition commands 316
 - filtering configuration 316
 - filtering port configuration 317
 - group information 67
 - group maintenance 392
 - mrouter maintenance commands 393
 - multicast group information 65
 - multicast
 - group information 65
 - multicast router information 68
 - snooping configuration 314
 - static mrouter configuration 318
 - statistics 164
- IGMPv3
 - configuration 315
 - information 67
 - snooping information 393
 - statistics 164
- image
 - downloading 372
 - software, selecting 373
- information
 - VMware 94
- Information Commands 25 to 123
- IP address
 - configuring default gateway 311
- IP forwarding
 - information 60
- IP Information 60, 72
- IP interfaces
 - configuring address 307
 - information 60
- IP network filter configuration 312
- IP statistics 152
- IPMC group information 68
- IPv6
 - ACL configuration 263
 - default gateway configuration 321
 - interface information 70
 - Neighbor Discovery

- cache information 64
- cache information commands 64
- cache manipulation 394
- configuration commands 308
- Path MTU
 - configuration 322
 - information 71
- re-marking
 - configuration 275
 - in-profile configuration 276
 - out-of-profile configuration 276
- routing information 62, 63
- statistics 155
- IPv6 route 160
- ISCLI command modes 18
- ISCLI commands
 - basics 17 to ??

J

- Japan Class A electronic emission statement 426
- Japan Electronics and Information Technology Industries Association statement 427
- JEITA statement 427

K

- Korea Class A electronic emission statement 427

L

- LACP
 - admin key
 - add to Auto Monitor 296
 - add to Backup interface 302
 - add to Manual Monitor Control 298
 - add to Manual Monitor Port 297
 - add to Master interface 301
 - add to VM group 336
 - aggregator information 47
 - and trunk hash configuration 288
 - configuration 292
 - information 47
 - port configuration 293
 - port status information 47
 - statistics 145, 146
- Layer 2 commands 43
- Layer 3 commands 60
- LDAP server configuration 212
- Lightweight Directory Access Protocol (see LDAP) 212
- Link Layer Discovery Protocol (see LLDP) 53
- link speed, configuring 244
- link status 25
 - command 83
 - duplex mode 25, 83
 - information 83
 - port speed 25, 83
- linkt (SNMP option) 218

- LLDP
 - cache manipulation commands 391
 - disable 282
 - enable 282
 - information 53
 - packets received 170
 - PDU's logged 175
 - remote device information 54
 - statistics 145, 148
 - TLV configuration 284
- log, syslog messaging options 202

M

- MAC address
 - display 26
 - FDB information 44
 - FDB maintenance 387
 - multicast, configuring 280
 - switch management processor 39
- MAC address spoof prevention 339
- Maintenance commands 385
- Management Processor (see MP) 26
- manual style conventions 14
- meter
 - ACL
 - configuring 272
 - current parameters 272
 - delete 272
 - port metering 268
- Miscellaneous Debug commands 389
- monitor port 277
- MP
 - display MAC address 26, 39
 - packet statistics 167
 - snap trace buffer 389
 - statistics 166
 - trace buffer 389
- Mrouter information 68
- MTU 322
- multicast
 - router information 68
 - static MAC configuration 280
- multiple management VLANs 303

N

- Neighbor Discovery
 - cache manipulation, IPv6 394
 - IPv6, configuration 308
- Network Configuration Protocol (NETCONF) 232
- New Zealand Class A statement 424
- notes, important 420
- notice 197
- notices 417
- NTP synchronization 214

O

OAM

- information 56
- statistics 128, 145, 149

online help 20

Operations commands 355

operations-level

- port commands 356

P

particulate contamination 422

passwords 23

- administrator account 23
- changing 233
- default 23
- user account 23

Path MTU 322

People's Republic of China Class A electronic emission statement 427

PFC configuration 325

ping 20

port

- ACL configuration 247
- configuration 238
- disabling temporarily 244
- Error Disable and Recovery 243
- failover manual monitor configuration 297
- FIPS configuration 329
- IGMP filtering configuration 317
- information 85
- LACP
 - configuration 293
 - status information 47
- link configuration 244
- link speed, configuring 244
- management, configuring 250
- membership of the VLAN 43, 59
- mirroring, configuring 277
- number 83
- reference 45
- speed 25, 83
- state information 45
- telnet 229
- TFTP 229
- trunking
 - configuration 286
 - description 286
- VLAN ID 25, 85
- port ECN configuration 248
- port WRED configuration 248
- preemption
 - hot links trigger, configuring 300
- Priority Flow Control 325
- Priority Groups
 - 802.1p mapping to 119
 - configuration 324
 - information 115

Private VLAN 305

Protected Mode 357

ptcfg (TFTP save command) 353

PVID (port VLAN ID) 25, 85

Q

QoS

- ACL parameters 247
- configuration 247, 251
- control plane protection 253
- DSCP configuration 252
- ECN information 76
- information 74
- transmit-queue information 75
- WRED information 76

R

RADIUS server

- configuration commands 206
- current parameters 207
- packets logged 175
- primary 206
- shared secret 206

receive flow control 244

reference ports 45

re-mark

- ACL
 - configuration 269, 273
 - parameters 78
- DSCP
 - configuration 238
 - global configuration 252
- in-profile
 - configuration 274
 - settings 269
- IPv6 ACL
 - configuration 275
 - in-profile configuration 276
 - out-of-profile configuration 276
 - parameters 276
- out-of-profile
 - configuration 274
 - settings 269
- TOS precedence, configuring 269
- user update priority 269

Remote Monitoring (RMON) 330

retries

- health checks for default gateway 311
- radius server 206

RMON

- configuration 330
- information 79

route statistics

- IPv6 160

Russia Class A electronic emission statement 427

S

- save (global command) 194
- secret, RADIUS server 206
- Secure Shell 204
- service and support
 - before you call 415
- shortcuts (CLI) 22
- SLP
 - configuration 351
 - information 101
 - statistics 190
- snap trace buffer 389
- SNMP
 - configuration
 - commands 217
 - current 219
 - link traps 218
 - location 218
 - read community string 218
 - source interface for traps 218
 - system authentication trap 217
 - system contact 217
 - timeout 218
 - trap host server 217
 - version 220
 - write community string 218
 - options 217
 - statistics 184
- SNMPv3
 - configuration
 - access rights 219
 - commands 219
 - community table 219, 225
 - destination 220
 - display 220
 - group 219, 224
 - MIB views 220
 - Notify table 228
 - parameters 220
 - target address table 226
 - target parameters 227
 - user access 223
 - user security 221
 - USM 220, 221
 - version 220
 - view 222
 - information 37
 - access 32
 - commands 29
 - community table 33
 - group 33
 - Notify table 36
 - target address table 34
 - target parameters table 35
 - USM user table 30
 - View Table 31

- software
 - image 372
 - image file and version 26, 39
- SPAR. *See* Switch Partition.
- static multicast MAC 280
- statistics
 - 160
 - ACL 181
 - bridging 129
 - commands 125 to 191
 - CPU 178
 - DNS 161
 - ethernet 130
 - FCoE 183
 - hot links 147
 - IGMP 164
 - interface 133
 - interface protocol 136
 - IPv4 152
 - IPv6 155
 - LACP 146
 - Layer 2 145
 - Layer 3 150
 - link 136
 - LLDP 148
 - logged packet 174
 - management processor 166
 - NTP 188
 - OAM 149
 - port 127
 - RMON 137
 - SNMP 184
 - TCP 161, 177
 - trunk group 144
 - UDP 163, 178
 - VMAP 182
- switch
 - name and location 26, 39
 - resetting 376
- Switch Partition (SPAR)
 - configuration 349
- Switch Partition (SPAR)
 - configuration 19
- system
 - date and time 26, 39
 - information 26, 39
- System Error Disable and Recovery 199

T

- tab completion (CLI) 22
- TACACS+ 208
- Taiwan Class A electronic emission statement 427
- TCP statistics 161, 177
- technical assistance 415

- telnet
 - configuring switches using 352
 - controlling access 229
 - port 229
 - radius server 206, 207, 212
- text conventions 14
- TFTP 372
 - port 229
 - PUT and GET commands 353
 - server 353
- timeout
 - idle connection 24
 - radius server 207
- TLV 284
- trace buffer 389
- traceroute 21
- trademarks 419
- transceiver status 86, 87
- Trunk group information 57
- trunk hash algorithm 288
- typographic conventions, manual 14

U

- UCB statistics 178
- UDLD
 - configuration 245
 - information 55
 - statistics 169, 174
- UDP statistics 163
- UFP. *See* Unified Fabric Port.
- UFP. *See* Universal Fabric Port.
- Unified Fabric Port (UFP)
 - configuration 343
- United States FCC Class A notice 424
- Universal Fabric Port (UFP)
 - configuration 19
- unknown (UNK) port state 45
- upgrade
 - switch software 372
- user access control configuration 233
- user account 23

V

- virtualization
 - configuration 334
 - information 88
- Virtualization Configuration 334
- VLAN
 - configuration 303
 - information 59
 - name 43, 59
 - Number 59
 - port membership 43, 59
 - setting access VLAN 240
 - setting default number (PVID) 240
 - tagging 85

- port configuration 239
- port restrictions 304
- port use of 25
- VLAN Map (see VMAP) 266
- VM
 - bandwidth management 335
 - Distributed Virtual Switch 361
 - Edge Virtual Bridge configuration 346
 - group configuration 336
 - information 92
 - policy configuration 335
 - profile configuration 340
 - VMready configuration 342
 - VMware
 - configuration 341
 - dvSwitch operations 361, 362
 - information 94
 - operations 359
- VM Check
 - configuration 337, 339, 341
- VMAP
 - configuration 266
 - definition 266
 - information 77
 - statistics 182
 - VLAN statistics 181
 - VMAP statistics 181
- VMware
 - configuration 341
 - distributed port group operations 362
 - dvSwitch administration 361
 - information 94
 - operations 359
- VSI
 - configuration mode 19

W

- watchdog timer 385
- weight
 - COS queue 74, 251
 - COS scheduling 75
- Weighted Random Early Detection (WRED) 255
- WRED (Weighted Random Early Detection) 255

Lenovo[™]

Part Number: 00MY385

Printed in USA

(IP) P/N: 00MY385