

IBM Flex System Fabric SI4093 System Interconnect Module



ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.7

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

First Edition (August 2013)

IBM Flex System Fabric SI4093 System Interconnect Module ISCLI Command Reference

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	ix
Who Should Use This Bookx
How This Book Is Organized	xi
Typographic Conventions	xii
Chapter 1. ISCLI Basics1
ISCLI Command Modes2
Global Commands4
Command Line Interface Shortcuts6
CLI List and Range Inputs6
Command Abbreviation6
Tab Completion6
User Access Levels7
Idle Timeout8
Chapter 2. Information Commands9
System Information	10
CLI Display Information	11
Error Disable and Recovery Information	12
SNMPv3 System Information	13
SNMPv3 USM User Table Information	14
SNMPv3 View Table Information	15
SNMPv3 Access Table Information	16
SNMPv3 Group Table Information	16
SNMPv3 Community Table Information	17
SNMPv3 Target Address Table Information	17
SNMPv3 Target Parameters Table Information	19
SNMPv3 Notify Table Information	19
SNMPv3 Dump Information	20
General System Information	21
Show Software Version Brief Information	22
Show Specific System Information	22
Show Recent Syslog Messages	22
User Status	24
Layer 2 Information	25
FDB Information	26
Show All FDB Information	26
Clearing Entries from the Forwarding Database	27
Link Aggregation Control Protocol Information	28
Link Aggregation Control Protocol	28
Layer 2 Failover Information Commands	29
Layer 2 Failover Information	29
LLDP Information	30
LLDP Remote Device Information	31
Unidirectional Link Detection Information	32
UDLD Port Information	32
OAM Discovery Information	33
OAM Port Information	33
Trunk Group Information	33
VLAN Information	35
Layer 3 Information	36

IPv6 Neighbor Discovery Cache Information	37
IPv6 Neighbor Discovery Cache Information	37
IPv6 Neighbor Discovery Prefix Information	38
Interface Information	38
IPv6 Interface Information	39
IPv6 Path MTU Information	39
IP Information	40
DHCP Snooping Binding Table Information	40
Quality of Service Information	41
Access Control List Information Commands	41
Access Control List Information	42
Link Status Information	42
Port Information	43
Port Transceiver Status	45
Converged Enhanced Ethernet Information	46
DCBX Information	46
DCBX Control Information	47
DCBX Feature Information	48
DCBX ETS Information	48
DCBX PFC Information	50
DCBX Application Protocol Information	51
ETS Information	53
PFC Information	54
FCoE Information	55
FIP Snooping Information	55
Information Dump	57
Chapter 3. Statistics Commands	59
Port Statistics	60
Bridging Statistics	61
Ethernet Statistics	62
Interface Statistics	65
Interface Protocol Statistics	67
Link Statistics	67
Trunk Group Statistics	68
Layer 2 Statistics	69
LACP Statistics	70
LLDP Port Statistics	71
OAM Statistics	72
Layer 3 Statistics	73
IPv4 Statistics	74
DNS Statistics	76
TCP Statistics	77
UDP Statistics	78
Management Processor Statistics	80
Packet Statistics	81
MP Packet Statistics	81
Packet Statistics Log	87
Packet Log example	87
Packet Statistics Last Packet	88
Packet Statistics Dump	88
Logged Packet Statistics	89
TCP Statistics	92

UDP Statistics	93
CPU Statistics	93
CPU Statistics History	96
Access Control List Statistics	97
ACL Statistics	98
Fibre Channel over Ethernet Statistics	99
SNMP Statistics	100
NTP Statistics	104
Statistics Dump	106
Chapter 4. Configuration Commands	107
Viewing and Saving Changes	108
System Configuration	109
System Error Disable and Recovery Configuration	112
System Host Log Configuration	113
SSH Server Configuration	115
RADIUS Server Configuration	116
TACACS+ Server Configuration	118
LDAP Server Configuration	121
NTP Server Configuration	123
System SNMP Configuration	125
SNMPv3 Configuration	127
User Security Model Configuration	129
SNMPv3 View Configuration	130
View-based Access Control Model Configuration	131
SNMPv3 Group Configuration	132
SNMPv3 Community Table Configuration	133
SNMPv3 Target Address Table Configuration	134
SNMPv3 Target Parameters Table Configuration	135
SNMPv3 Notify Table Configuration	136
System Access Configuration	137
Management Network Configuration	138
User Access Control Configuration	140
System User ID Configuration	141
Strong Password Configuration	142
Custom Daylight Saving Time Configuration	143
Port Configuration	144
Port Error Disable and Recovery Configuration	146
Port Link Configuration	147
Temporarily Disabling a Port	147
Unidirectional Link Detection Configuration	148
Port OAM Configuration	149
Port ACL Configuration	149
Port WRED Configuration	150
Port WRED Transmit Queue Configuration	150
Management Port Configuration	151
Quality of Service Configuration	153
Control Plane Protection	153
Weighted Random Early Detection Configuration	153
WRED Transmit Queue Configuration	154
Access Control Configuration	155
Access Control List Configuration	156
Ethernet Filtering Configuration	157

IPv4 Filtering Configuration	158
TCP/UDP Filtering Configuration	159
Packet Format Filtering Configuration	160
ACL IPv6 Configuration	160
IPv6 Filtering Configuration	161
IPv6 TCP/UDP Filtering Configuration	162
IPv6 Re-Mark Configuration	163
ACL Group Configuration	164
ACL Metering Configuration	164
ACL Re-Mark Configuration	165
Re-Marking In-Profile Configuration	166
Re-Marking Out-of-Profile Configuration	166
IPv6 Re-Marking Configuration	167
IPv6 Re-Marking In-Profile Configuration	168
Layer 2 Configuration	169
Forwarding Database Configuration	169
Static FDB Configuration	170
LLDP Configuration	170
LLDP Port Configuration	171
LLDP Optional TLV configuration	173
Trunk Configuration	175
IP Trunk Hash Configuration	176
Layer 2 Trunk Hash	176
Layer 3 Trunk Hash	177
Link Aggregation Control Protocol Configuration	178
LACP Port Configuration	179
Layer 2 Failover Configuration	180
Failover Trigger Configuration	180
Failover Manual Monitor Port Configuration	181
Failover Manual Monitor Control Configuration	182
Layer 3 Configuration	183
IP Interface Configuration	184
Default Gateway Configuration	186
Network Filter Configuration	187
Domain Name System Configuration	188
IPv6 Default Gateway Configuration	189
IPv6 Path MTU Configuration	189
IPv6 Neighbor Discovery Prefix Configuration	190
IPv6 Prefix Policy Table Configuration	191
Converged Enhanced Ethernet Configuration	192
ETS Global Configuration	193
ETS Global Priority Group Configuration	193
Priority Flow Control Configuration	194
Port-level 802.1p PFC Configuration	194
DCBX Port Configuration	195
Fibre Channel over Ethernet Configuration	197
FIPS Port Configuration	198
Switch Partition (SPAR) Configuration	199
Service Location Protocol Configuration	200
Configuration Dump	202
Saving the Active Switch Configuration	203
Restoring the Active Switch Configuration	204

Chapter 5. Operations Commands205
Operations-Level Port Commands206
Operations-Level FCoE Commands207
Protected Mode Options208
Chapter 6. Boot Options211
Scheduled Reboot211
Netboot Configuration212
QSFP Port Configuration213
Updating the Switch Software Image214
Loading New Software to Your Switch214
Selecting a Software Image to Run215
Uploading a Software Image from Your Switch215
Selecting a Configuration Block217
Resetting the Switch218
Changing the Switch Profile219
Using the Boot Management Menu220
Recovering from a Failed Software Upgrade220
Recovering a Failed Boot Image222
Chapter 7. Maintenance Commands225
Forwarding Database Maintenance227
Debugging Commands228
LLDP Cache Manipulation230
Uuencode Flash Dump231
TFTP or FTP System Dump Put232
Clearing Dump Information233
Unscheduled System Dumps234
Appendix A. IBM Networking OS System Log Messages.235
LOG_ALERT236
LOG_CRIT238
LOG_ERR239
LOG_INFO240
LOG_NOTICE243
LOG_WARNING247
Appendix B. Getting help and technical assistance249
Before you call250
Using the documentation251
Getting help and information on the World Wide Web252
Software service and support253
Hardware service and support254
IBM Taiwan product service255
Index257

Preface

The *IBM Flex System Fabric SI4093 System Interconnect Module ISCLI Command Reference* describes how to configure and use the IBM Networking OS 7.7 software with your IBM Flex System Fabric SI4093 System Interconnect Module. 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 *IBM N/OS 7.7 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, “IBM Networking OS System Log Messages,” lists IBM Networking 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 IBM products.

“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	<p>This type is used for names of commands, files, and directories used within the text. For example:</p> <p>View the <code>readme.txt</code> file.</p> <p>It also depicts on-screen computer output and prompts.</p>
bold fixed-width text	<p>This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example:</p> <p><code>show sys-info</code></p>
bold body text	<p>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.</p>
<i>italicized body text</i>	<p>This italicized type indicates book titles, special terms, or words to be emphasized.</p>
angle brackets < >	<p>Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is</p> <pre>ping <IP address></pre> <p>you enter</p> <pre>ping 192.32.10.12</pre>
braces { }	<p>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.</p> <p>Example: If the command syntax is</p> <pre>show portchannel {<I-64> hash information}</pre> <p>you enter:</p> <pre>show portchannel <I-64></pre> <p>or</p> <pre>show portchannel hash</pre> <p>or</p> <pre>show portchannel information</pre>

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 <code>show interface ip [<1-4>]</code></p> <p>you enter <code>show interface ip</code></p> <p>or <code>show interface ip <1-4></code></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 <code>show portchannel {<1-64> hash information}</code></p> <p>you must enter: <code>show portchannel <1-64></code></p> <p>or <code>show portchannel hash</code></p> <p>or <code>show portchannel information</code></p>

Chapter 1. ISCLI Basics

Your SI4093 10Gb 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](#).

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 Router>	Default mode, entered automatically on console Exit: <code>exit</code> or <code>logout</code>
Privileged EXEC Router#	Enter Privileged EXEC mode, from User EXEC mode: <code>enable</code> Exit to User EXEC mode: <code>disable</code> Quit ISCLI: <code>exit</code> or <code>logout</code>
Global Configuration Router(config)#	Enter Global Configuration mode, from Privileged EXEC mode: <code>configure terminal</code> Exit to Privileged EXEC: <code>end</code> or <code>exit</code>
Interface IP Router(config-ip-if)#	Enter Interface IP Configuration mode, from Global Configuration mode: <code>interface ip <interface number></code> Exit to Global Configuration mode: <code>exit</code> Exit to Privileged EXEC mode: <code>end</code>
Interface Port Router(config-if)#	Enter Port Configuration mode, from Global Configuration mode: <code>interface port <port number or alias></code> Exit to Privileged EXEC mode: <code>exit</code> Exit to Global Configuration mode: <code>end</code>

Table 1. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Interface PortChannel Router(config-PortChannel)#	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: interface portchannel {<trunk number> lacp <key>} Exit to Privileged EXEC mode: exit Exit to Global Configuration mode: end
VLAN Router(config-vlan)#	Enter VLAN Configuration mode, from Global Configuration mode: vlan <VLAN number> Exit to Global Configuration mode: exit Exit to Privileged EXEC mode: end
SPAR Configuration SI4093(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
?	Provides more information about a specific command or lists commands available at the current level.
list	Lists the commands available at the current level.
exit	Go up one level in the command mode structure. If already at the top level, exit from the command line interface and log out.
copy running-config startup-config	Write configuration changes to non-volatile flash memory.
logout	Exit from the command line interface and log out.
ping	<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"> – -n: Sets the number of attempts (optional). – -w: Sets the number of milliseconds between attempts (optional). – -l: Sets the ping request payload size (optional). – -s: Sets the IP source address for the IP packet (optional). – -v: Sets the Type Of Service bits in the IP header. – -f: Sets the <i>don't fragment</i> bit in the IP header (only for IPv4 addresses). – -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> <pre>tracert {<hostname> <IP address>} [<max-hops (1-32)> [<msec delay>]]</pre> <pre>tracert <hostname> <IP address> [<max-hops (1-32)> [<msec-delay (1-4294967295)>]]</pre> <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 <code>ping</code>, 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> <pre>telnet {<hostname> <IP address>} [<port>]</pre> <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:

<code># vlan 1,3,4095</code>	<i>(access VLANs 1, 3, and 4095)</i>
<code># vlan 1-20</code>	<i>(access VLANs 1 through 20)</i>
<code># vlan 1-5,90-99,4090-4095</code>	<i>(access multiple ranges)</i>
<code># vlan 1-5,19,20,4090-4095</code>	<i>(access a mix of lists and ranges)</i>

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:

<code># interface port 1-4</code>	<i>(Access ports 1 through 4)</i>
-----------------------------------	-----------------------------------

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:

<code>Router(config)# spanning-tree stp 2 bridge hello 2</code>
or
<code>Router(config)# sp stp 2 br h 2</code>

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.	user
Operator	The Operator can make temporary changes that are lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations.	
Administrator	The superuser Administrator has complete access to all command modes, information, and configuration commands on the SI4093 10Gb System Interconnect Module, 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
<pre>show interface status <port alias or number></pre> <p>Displays configuration information about the selected port(s), including:</p> <ul style="list-style-type: none">– Port alias and number– Port speed– Duplex mode (half, full, or auto)– Flow control for transmit and receive (no, yes, or both)– Link status (up, down, or disabled) <p>For details, see page 42.</p> <p>Command mode: All</p>
<pre>show interface trunk <port alias or number></pre> <p>Displays port status information, including:</p> <ul style="list-style-type: none">– Port alias and number– Whether the port uses VLAN Tagging or not– Port VLAN ID (PVID)– Port name– VLAN membership– FDB Learning status– Flooding status <p>For details, see page 43.</p> <p>Command mode: All</p>
<pre>show interface transceiver</pre> <p>Displays the status of the port transceiver module on each external port. For details, see page 45.</p> <p>Command mode: All</p>
<pre>show information-dump</pre> <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 10](#), with pointers to where detailed information can be found.

Table 5. System Information Commands

Command Syntax and Usage
<pre>show sys-info</pre> <p>Displays system information, including:</p> <ul style="list-style-type: none">– System date and time– Switch model name and number– Switch name and location– Time of last boot– MAC address of the switch management processor– IP address of management interface– Hardware version and part number– Software image file and version number– Configuration name– Log-in banner, if one is configured– Internal temperatures <p>For details, see page 21.</p> <p>Command mode: All</p>
<pre>show logging [severity <0-7>] [reverse]</pre> <p>Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the <code>show logging messages</code> command. For details, see page 22.</p> <p>Command mode: All</p>
<pre>show access user</pre> <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
<pre>show terminal-length</pre> <p>Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled.</p> <p>Command mode: All</p>
<pre>show line console length</pre> <p>Displays the current line console length setting. For details, see page 109.</p> <p>Command mode: All</p>
<pre>show line vty length</pre> <p>Displays the current line vty length setting. For details, see page 109.</p> <p>Command mode: All</p>

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
<code>show errdisable recovery</code> Displays a list ports with their Error Recovery status. Command mode: All
<code>show errdisable timers</code> Displays a list of active recovery timers, if applicable. Command mode: All
<code>show errdisable information</code> Displays all Error Disable and Recovery information. Command mode: All

SNMPv3 System Information

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

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

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

Table 8. SNMPv3 Commands

Command Syntax and Usage
<pre>show snmp-server v3 user</pre> <p>Displays User Security Model (USM) table information. To view the table, see page 14.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 view</pre> <p>Displays information about view, subtrees, mask and type of view. To view a sample, see page 15.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 access</pre> <p>Displays View-based Access Control information. To view a sample, see page 16.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 group</pre> <p>Displays information about the group, including the security model, user name, and group name. To view a sample, see page 16.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 community</pre> <p>Displays information about the community table information. To view a sample, see page 17.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 target-address</pre> <p>Displays the Target Address table information. To view a sample, see page 17.</p> <p>Command mode: All</p>
<pre>show snmp-server v3 target-parameters</pre> <p>Displays the Target parameters table information. To view a sample, see page 19.</p> <p>Command mode: All</p>

Table 8. SNMPv3 Commands (continued)

Command Syntax and Usage
<pre>show snmp-server v3 notify</pre> <p>Displays the Notify table information. To view a sample, see page 19.</p> <p>Command mode: All</p>
<pre>show snmp-server v3</pre> <p>Displays all the SNMPv3 information. To view a sample, see page 20.</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. IBM Networking OS supports DES algorithm for privacy. The software also supports two authentication algorithms: MD5 and HMAC-SHA.

SNMPv3 View Table Information

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

The following command displays the SNMPv3 View Table:

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

Command mode: All

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

Table 10. SNMPv3 View Table Information Parameters

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

SNMPv3 Access Table Information

The access control subsystem provides authorization services.

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

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

The following command displays SNMPv3 access information:

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

Command mode: All

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

Table 11. SNMPv3 Access Table Information

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

SNMPv3 Group Table Information

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

The following command displays SNMPv3 group information:

```
show snmp-server v3 group
```

Command mode: All

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

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 <code>snmpTargetAddrEntry</code> .
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 <code>snmpTargetParamsTable</code> . 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 <code>snmpTargetParamsEntry</code> .
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the <code>securityName</code> , 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 <code>inconsistentValue</code> 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 <code>snmpNotifyEntry</code> .
Tag	This represents a single tag value which is used to select entries in the <code>snmpTargetAddrTable</code> . Any entry in the <code>snmpTargetAddrTable</code> 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:
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 16:50:45 Wed Nov 16, 2011
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

IBM Flex System Fabric SI4093 System Interconnect Module for IBM BladeCenter

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2010 (reset from console)

PCBA Part Number:      BAC-00042-00
Hardware Part Number:  46C7193
FAB Number:            BN-RZZ000
Serial Number:         PROTO2C04E
Manufacturing Date:    43/08
Hardware Revision:     0
Board Revision:        1
PLD Firmware Version:  4.0

Temperature Sensor 1 (Warning): 42.0 C (Warn at 88.0 C/Recover at 78.0 C)
Temperature Sensor 2 (Shutdown): 42.5 C (Shutdown at 98.0 C/Recover at 88.0 C)
Temperature Sensor 3 (Exhaust): 37.5 C
Temperature Sensor 4 (Inlet):  32.5 C
```

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 Information

The following command displays brief software version information:

```
show version brief
```

Command mode: All

```
Software Version 7.7.1.0 (FLASH image2), active configuration.
```

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

Show Specific System Information

[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
<pre>show version brief</pre> <p>Displays the software version number, image file, and configuration name.</p> <p>Command mode: All</p>

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

Date	Time	Criticality level	Message
Jul 8	17:25:41	NOTICE	system: link up on port 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.

User Status

The following command displays user status information:

```
show access user
```

Command mode: All except User EXEC

```
Username:
  user      - enabled - offline
  oper      - disabled - offline
  admin     - Always Enabled - online 1 session
Current User ID table:
  1: name paul      , dis, cos user      , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

Layer 2 Information

The following commands display Layer 2 information.

Table 18. Layer 2 Information Commands

Command Syntax and Usage
<pre>show portchannel information</pre> <p>Displays the state of each port in the various static or LACP trunk groups. For details, see page 33.</p> <p>Command mode: All</p>
<pre>show vlan</pre> <p>Displays VLAN configuration information for all configured VLANs, including:</p> <ul style="list-style-type: none">– VLAN Number– VLAN Name– Status– Port membership of the VLAN <p>For details, see page 35.</p> <p>Command mode: All</p>
<pre>show failover trigger <trigger number></pre> <p>Displays Layer 2 Failover information. For details, see page 29.</p> <p>Command mode: All</p>
<pre>show layer2 information</pre> <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 K MAC address entries on the MP per switch.

Table 19. FDB Information Commands

Command Syntax and Usage
<pre>show mac-address-table address <MAC address></pre> <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, xxxxxxxxxxxxxx. For example, 080020123456</p> <p>Command mode: All</p>
<pre>show mac-address-table interface port <port alias or number></pre> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All</p>
<pre>show mac-address-table vlan <VLAN number></pre> <p>Displays all FDB entries on a single VLAN.</p> <p>Command mode: All</p>
<pre>show mac-address-table state {unknown forward trunk}</pre> <p>Displays all FDB entries for a particular state.</p> <p>Command mode: All</p>
<pre>show mac-address-table static</pre> <p>Displays all static MAC entries in the FDB.</p> <p>Command mode: All</p>
<pre>show mac-address-table configured static</pre> <p>Displays all configured static MAC entries in the FDB.</p> <p>Command mode: All</p>
<pre>show mac-address-table</pre> <p>Displays all entries in the Forwarding Database.</p> <p>Command mode: All</p> <p>For more information, see page 26.</p>

Show All FDB Information

The following command displays Forwarding Database information:

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


Command mode: All

MAC address	VLAN	Port	Trnk	State	Permanent
00:04:38:90:54:18	1	EXT4		FWD	
00:09:6b:9b:01:5f	1	INT13		FWD	
00:09:6b:ca:26:ef	4095	MGT1		FWD	
00:0f:06:ec:3b:00	4095	MGT1		FWD	
00:11:43:c4:79:83	1	EXT4		FWD	P

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address.

When an address is in the unknown state, no outbound port is indicated, although ports that reference the address as a destination will be listed under "Reference ports."

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to ["Forwarding Database Maintenance"](#) on page 227.

Link Aggregation Control Protocol Information

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

Table 20. LACP Information Commands

Command Syntax and Usage
<pre>show lacp aggregator <aggregator ID></pre> <p>Displays detailed information about the LACP aggregator.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> lacp information</pre> <p>Displays LACP information about the selected port.</p> <p>Command mode: All</p>
<pre>show lacp information</pre> <p>Displays a summary of LACP information.</p> <p>Command mode: All</p> <p>For details, see page 28.</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
1	off	1	1	no	32768	--	--	--	1
2	off	2	2	no	32768	--	--	--	1
3	off	3	3	no	32768	--	--	--	1
...									

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.
- **prio** Shows the value of the port priority.
- **aggr** Displays the aggregator associated with each port.
- **trunk** This value represents the LACP trunk group number.
- **status** Displays the status of LACP on the port (up, down or standby).
- **minlinks** Displays the minimum number of active links in the LACP trunk.

Layer 2 Failover Information Commands

Table 21. Layer 2 Failover Information Commands

Command Syntax and Usage
<pre>show failover trigger <trigger number></pre> <p>Displays detailed information about the selected Layer 2 Failover trigger.</p> <p>Command mode: All</p>
<pre>show failover trigger</pre> <p>Displays a summary of Layer 2 Failover information. For details, see page 29.</p> <p>Command mode: All</p>

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

```
show failover trigger
```

Command mode: All

<pre>Trigger 1 Auto Monitor: Enabled Trigger 1 limit: 0 Monitor State: Up Member Status ----- trunk 1 EXT2 Operational EXT3 Operational Control State: Auto Disabled Member Status ----- INT1 Operational INT2 Operational INT3 Operational INT4 Operational ... </pre>
--

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 trunk group, the port is aggregated.

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

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

A control port's status is displayed as `Failed` only if the monitor trigger state is `Down`.

LLDP Information

The following commands display LLDP information.

Table 22. LLDP Information Commands

Command Syntax and Usage
<pre>show lldp port</pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p>Command mode: All</p>
<pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p>Command mode: All</p>
<pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p>Command mode: All</p>
<pre>show lldp remote-device [<1-256> detail]</pre> <p>Displays information received from LLDP-capable devices. To view a sample display, see page 31.</p>
<pre>show lldp information</pre> <p>Displays all LLDP information.</p> <p>Command mode: All</p>

LLDP Remote Device Information

The following command displays LLDP remote device information:

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

Command mode: All

LLDP Remote Devices Information				
LocalPort	Index	Remote Chassis ID	RemotePort	Remote System Name
MGT	210	00 16 ca ff 7e 00	15	BNT Gb Ethernet Switch...
EXT4	15	00 16 60 f9 3b 00	20	BNT Gb Ethernet Switch...

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

Local Port Alias: EXT1	
Remote Device Index	: 15
Remote Device TTL	: 99
Remote Device RxChanges	: false
Chassis Type	: Mac Address
Chassis Id	: 00-18-b1-33-1d-00
Port Type	: Locally Assigned
Port Id	: 23
Port Description	: EXT1
System Name :	
System Description : IBM Networking Operating System IBM Flex System Fabric SI4093 System Interconnect Module, IBM Networking OS: version 7.6.1,0 Boot image: version 7.7.1	
System Capabilities Supported : bridge, router	
System Capabilities Enabled : bridge, router	
Remote Management Address:	
Subtype	: IPv4
Address	: 10.100.120.181
Interface Subtype	: ifIndex
Interface Number	: 128
Object Identifier	:

Unidirectional Link Detection Information

The following commands show unidirectional link detection information.

Table 23. UDLD Information Commands

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

UDLD Port Information

The following command displays UDLD information for the selected port:

```
show interface port <port alias or number> udld
```

Command mode: All

<pre>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</pre>

UDLD information includes the following:

- Status (enabled or disabled)
- Mode (normal or aggressive)
- Port state (link up or link down)
- Bi-directional status (unknown, unidirectional, bidirectional, TX-RX loop, neighbor mismatch)

OAM Discovery Information

Table 24. OAM Discovery Information Commands

Command Syntax and Usage
<pre>show interface port <port alias or number> oam</pre> <p>Displays OAM information about the selected port.</p> <p>Command mode: All</p>
<pre>show oam</pre> <p>Displays all OAM information.</p> <p>Command mode: All</p>

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.

Trunk Group Information

The following command displays Trunk Group information:

```
show portchannel information
```

Command mode: All

```
Trunk group 1: Enabled
Protocol - Static
Port state:
  EXT1: STG 1 forwarding
  EXT2: STG 1 forwarding
```

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

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

VLAN Information

Table 25. VLAN Information Commands

Command Syntax and Usage
<pre>show vlan <VLAN number></pre> <p>Displays general VLAN information.</p>
<pre>show vlan information</pre> <p>Displays information about all VLANs, including:</p> <ul style="list-style-type: none"> – VLAN number and name – Port membership – VLAN status (enabled or disabled) – Protocol VLAN status – Private VLAN status – Spanning Tree membership –

The following command displays VLAN information:

```
show vlan <VLAN number>
```

Command mode: All

VLAN	Name	Status	MGT	Ports
1	Default VLAN	ena	dis	INT1A-INT14B EXT1-EXT10 EXT15-EXT22
4095	Mgmt VLAN	ena	ena	MGT1 EXTM

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of BladeCenter unit 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
- Status
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

Layer 3 Information

Table 26. Layer 3 Information Commands

Command Syntax and Usage
<pre>show ipv6 neighbors</pre> <p>Displays IPv6 Neighbor Discovery cache information. For more information options, see page 37.</p> <p>Command mode: All</p>
<pre>show ipv6 prefix</pre> <p>Displays IPv6 Neighbor Discovery prefix information. For details, see page 38.</p> <p>Command mode: All</p>
<pre>show interface ip</pre> <p>Displays IPv4 interface information. For details, see page 38.</p> <p>Command mode: All</p>
<pre>show ipv6 interface <interface number></pre> <p>Displays IPv6 interface information. For details, see page 39.</p> <p>Command mode: All</p>
<pre>show ipv6 pmtu [<destination IPv6 address>]</pre> <p>Displays IPv6 Path MTU information. For details, see page 39.</p> <p>Command mode: All</p>
<pre>show ip interface brief</pre> <p>Displays IP information. For details, see page 40.</p> <p>IP information, includes:</p> <ul style="list-style-type: none">– IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status.– Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status– IP forwarding settings, network filter settings, route map settings <p>Command mode: All</p>
<pre>show layer3</pre> <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>

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

IPv6 Neighbor Discovery Cache Information

Table 27. IPv6 Neighbor Discovery Cache Information Commands

Command Syntax and Usage
<pre>show ipv6 neighbors find <IPv6 address></pre> <p>Shows a single IPv6 Neighbor Discovery cache entry by IP address. Command mode: All</p>
<pre>show ipv6 neighbors interface port <port alias or number></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single port. Command mode: All</p>
<pre>show ipv6 neighbors vlan <VLAN number></pre> <p>Shows IPv6 Neighbor Discovery cache entries on a single VLAN. Command mode: All</p>
<pre>show ipv6 neighbors static</pre> <p>Displays static IPv6 Neighbor Discovery cache entries. Command mode: All</p>
<pre>show ipv6 neighbors</pre> <p>Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 37. 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

IPv6 Neighbor Discovery Prefix Information

The following command displays a summary of IPv6 Neighbor Discovery prefix information:

```
show ipv6 prefix
```

Command mode: All

```
Codes: A - Address , P - Prefix-Advertisement
       D - Default , N - Not Advertised
       [L] - On-link Flag is set
       [A] - Autonomous Flag is set

AD 10:: 64 [LA] Valid lifetime 2592000 , Preferred lifetime 604800
P 20:: 64 [LA] Valid lifetime 200 , Preferred lifetime 100
```

Neighbor Discovery prefix information includes information about all configured prefixes.

Interface Information

The following command displays interface information:

```
show interface ip
```

Command mode: All

```
Interface information:
 1: IP4 172.31.35.5      255.255.0.0 172.31.255.255, vlan 1, up
128: IP4 10.90.90.97   255.255.255.0 10.90.90.255, vlan 4095, up
```

For each interface, the following information is displayed:

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

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 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

DHCP Snooping Binding Table Information

The following command displays the DHCP binding table:

```
show ip dhcp snooping binding
```

Command mode: All

Mac Address	IP Address	Lease(seconds)	Type	VLAN	Interface
00:00:01:00:02:01	10.0.0.1	1600	dynamic	100	port 1
02:1c:5f:d1:18:9c	210.38.197.63	86337	Static	127	1
06:51:4d:e6:16:2d	194.116.155.190	86337	Static	105	1
08:69:0f:1d:ba:3d	40.90.17.26	86337	Static	150	1
08:a2:6d:00:36:56	40.194.18.213	86337	Static	108	1
0e:a7:f8:a2:74:2c	130.254.47.129	86337	Static	171	1
0e:b7:64:02:97:7c	35.92.27.110	86337	Static	249	1
0e:f7:5b:6a:74:d8	75.179.93.39	86337	Static	232	1

Total number of bindings: 8

The DHCP Snooping binding table displays information for each entry in the table. Each entry has a MAC address, an IP address, the lease time, the interface to which the entry applies, and the VLAN to which the interface belongs.

Quality of Service Information

Table 28. QoS Information Options

Command Syntax and Usage
<pre>show qos random-detect</pre> <p>Displays WRED ECN information.</p> <p>Command mode: All</p>

Access Control List Information Commands

Table 29. ACL Information Options

Command Syntax and Usage
<pre>show access-control list <ACL number></pre> <p>Displays ACL list information. For details, see page 42.</p> <p>Command mode: All</p>
<pre>show access-control list6 <ACL number></pre> <p>Displays IPv6 ACL list information.</p> <p>Command mode: All</p>
<pre>show access-control group <ACL group number></pre> <p>Displays ACL group information.</p> <p>Command mode: All</p>

Access Control List Information

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

```
show access-control list <ACL number>
```

Command mode: All

```
Current ACL information:
-----
Filter 2 profile:
 Ethernet
  - VID      : 2/0xffff
  Actions    : Permit
  Statistics  : enabled
```

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

Table 30. ACL Parameter Descriptions

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

Link Status Information

The following command displays link information:

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

Command mode: All

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 BladeCenter unit 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 Trk	Type	Lrn	Fld	PVID	DESCRIPTION	VLAN(s)
INT1	1	y	Internal	e	e	1	INT1	1 4095
INT2	2	y	Internal	e	e	1	INT2	1 4095
INT3	3	y	Internal	e	e	1	INT3	1 4095
INT4	4	y	Internal	e	e	1	INT4	1 4095
INT5	5	y	Internal	e	e	1	INT5	1 4095
INT6	6	y	Internal	e	e	1	INT6	1 4095
INT7	7	y	Internal	e	e	1	INT7	1 4095
INT8	8	y	Internal	e	e	1	INT8	1 4095
INT9	9	y	Internal	e	e	1	INT9	1 4095
INT10	10	y	Internal	e	e	1	INT10	1 4095
INT11	11	y	Internal	e	e	1	INT11	1 4095
INT12	12	y	Internal	e	e	1	INT12	1 4095
ISL1	13	n	Isl	e	e	1	ISL1	1
ISL2	14	n	Isl	e	e	1	ISL2	1
MGT1	15	y	Mgmt	e	e	4095*	MGT1	4095
MGT2	16	y	Mgmt	e	e	4095*	MGT2	4095
EXT1	17	n	External	e	e	1	EXT1	1
EXT2	18	n	External	e	e	2	EXT2	2
EXT3	19	n	External	e	e	1	EXT3	1
EXT4	20	n	External	e	e	1	EXT4	1
EXT5	21	n	External	e	e	1	EXT5	1
EXT6	22	n	External	e	e	1	EXT6	1
EXT7	23	n	External	e	e	1	EXT7	1
EXT8	24	n	External	e	e	1	EXT8	1
EXT9	25	n	External	e	e	1	EXT9	1
EXT10	26	n	External	e	e	1	EXT10	1
EXT11	27	n	External	e	e	1	EXT11	1

* = 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 BladeCenter unit 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 is internal, external or used for management
- Whether the port has FDB Learning enabled (Lrn)
- Whether the port has Port Flooding enabled (Fld)
- Port VLAN ID (PVID)
- 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

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

- Port number and media type
- TX: Transmission status
- RXlos: Receive Loss of Signal indicator
- TXflt: Transmission fault indicator
- Volts: Power usage, in volts
- DegsC: Temperature, in degrees centigrade
- TXuW: Transmit power, in micro-watts
- RXuW: Receive power, in micro-watts
- Media type (LX, LR, SX, SR)
- Laser wavelength, in nano-meters
- Approval status

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

Table 31. 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.

Converged Enhanced Ethernet Information

[Table 32](#) describes the Converged Enhanced Ethernet (CEE) information options.

Table 32. CEE Information Options

Command Syntax and Usage
<pre>show cee information</pre> <p>Displays all CEE information</p> <p>Command mode: All</p>

DCBX Information

[Table 33](#) describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 33. DCBX Information Options

Command Syntax and Usage
<pre>show cee information dcbx port <port alias or number> control</pre> <p>Displays information about the DCBX Control state machine for the selected port. For details, see page 47.</p> <p>Command mode: All</p>
<pre>show cee information dcbx port <port alias or number> feature</pre> <p>Displays information about the DCBX Feature state machine for the selected port. For details, see page 48.</p> <p>Command mode: All</p>
<pre>show cee information dcbx port <port alias or number> ets</pre> <p>Displays information about the DCBX ETS state machine. For details, see page 48.</p> <p>Command mode: All</p>
<pre>show cee information dcbx port <port alias or number> pfc</pre> <p>Displays information about the DCBX PFC state machine. For details, see page 50.</p> <p>Command mode: All</p>
<pre>show cee information dcbx port <port alias or number> app_proto</pre> <p>Displays information about the DCBX Application Protocol state machine on the selected port. For details, see page 51.</p> <p>Command mode: All</p>
<pre>show cee information dcbx port <port alias or number></pre> <p>Displays all DCBX information.</p> <p>Command mode: All</p>

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 34. 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 35. 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 36. 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"> - 0 = Ethernet Type - 1 = TCP socket ID
Organizationally Unique ID	DCBX TLV identifier

Table 36. 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 37](#) describes the Enhanced Transmission Selection (ETS) information options

Table 37. ETS Information Options

Command Syntax and Usage
<pre>show cee global ets information</pre> <p>Displays global ETS information.</p> <p>Command mode: All</p>

The following command displays ETS information:

```
show cee global ets information
```

Command mode: All

<pre>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</pre>
--

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 38](#) describes the Priority Flow Control (PFC) information options.

Table 38. PFC Information Options

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

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																														
<table><thead><tr><th>Priority</th><th>State</th><th>Description</th></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr></thead><tbody><tr><td>0</td><td>Dis</td><td></td></tr><tr><td>1</td><td>Dis</td><td></td></tr><tr><td>2</td><td>Dis</td><td></td></tr><tr><td>3</td><td>Ena</td><td></td></tr><tr><td>4</td><td>Dis</td><td></td></tr><tr><td>5</td><td>Dis</td><td></td></tr><tr><td>6</td><td>Dis</td><td></td></tr><tr><td>7</td><td>Dis</td><td></td></tr></tbody></table>	Priority	State	Description	-----	-----	-----	0	Dis		1	Dis		2	Dis		3	Ena		4	Dis		5	Dis		6	Dis		7	Dis	
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 39](#) describes the Fibre Channel over Ethernet (FCoE) information options.

Table 39. FCoE Information Options

Command Syntax and Usage
<pre>show fcoe information</pre> <p>Displays all current FCoE information.</p> <p>Command mode: All</p>

FIP Snooping Information

[Table 40](#) describes the Fibre Channel Initialization Protocol (FIP) Snooping information options

Table 40. FIP Snooping Information Options

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

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

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

Command mode: All

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

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

FIP Snooping port information includes the following:

- 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 41. Statistics Commands

Command Syntax and Usage
<pre>show layer3 counters</pre> <p>Command mode: All Displays Layer 3 statistics.</p>
<pre>show snmp-server counters</pre> <p>Command mode: All Displays SNMP statistics. See page 100 for sample output.</p>
<pre>show ntp counters</pre> <p>Displays Network Time Protocol (NTP) Statistics. Command mode: All See page 104 for a sample output and a description of NTP Statistics.</p>
<pre>show counters</pre> <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. Command mode: All For details, see page 106.</p>

Port Statistics

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

Table 42. Port Statistics Commands

Command Syntax and Usage
<pre>show interface port <port alias or number> bridging-counters</pre> <p>Displays bridging (“dot1”) statistics for the port. See page 61 for sample output.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> ethernet-counters</pre> <p>Displays Ethernet (“dot3”) statistics for the port. See page 62 for sample output.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> interface-counters</pre> <p>Displays interface statistics for the port. See page 65 for sample output.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> ip-counters</pre> <p>Displays IP statistics for the port. See page 67 for sample output.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> link-counters</pre> <p>Displays link statistics for the port. See page 67 for sample output.</p> <p>Command mode: All</p>
<pre>show interface port <port alias or number> oam counters</pre> <p>Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port.</p> <p>Command mode: All</p>
<pre>clear interface port <port alias or number> counters</pre> <p>Clears all statistics for the port.</p> <p>Command mode: All except User EXEC</p>
<pre>clear counters</pre> <p>Clears statistics for all ports.</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 43. 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 44. 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 44. Ethernet Statistics for Port (continued)

Statistics	Description
dot3StatsSingleCollisionFrames	<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>
dot3StatsMultipleCollisionFrames	<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>
dot3StatsExcessiveCollisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMacTransmitErrors	<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 44. 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 45. 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 45. 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 <code>pause</code> 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.

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 46. 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 47. Link Statistics

Statistics	Description
linkStateChange	The total number of link state changes.

Trunk Group Statistics

Table 48. Trunk Group Statistics Commands

Command Syntax and Usage
<pre>show interface portchannel <trunk group number> interface counters</pre> <p>Displays interface statistics for the trunk group.</p> <p>Command mode: All</p>
<pre>clear interface portchannel <trunk group number> counters</pre> <p>Clears all the statistics on the specified trunk group.</p> <p>Command mode: All except User EXEC</p>

Layer 2 Statistics

Table 49. Layer 2 Statistics Commands

Command Syntax and Usage
<pre>show interface port <port alias or number> lacp counters</pre> <p>Displays Link Aggregation Control Protocol (LACP) statistics. See page 70 for sample output.</p> <p>Command mode: All</p>
<pre>clear interface port <port alias or number> lacp counters</pre> <p>Clears Link Aggregation Control Protocol (LACP) statistics.</p> <p>Command mode: All except User EXEC</p>
<pre>show interface port <port alias or number> lldp counters</pre> <p>Displays LLDP statistics. See page 71 for sample output.</p> <p>Command mode: All except User EXEC</p>
<pre>show oam counters</pre> <p>Displays OAM statistics. See page 72 for sample output.</p> <p>Command mode: All except User EXEC</p>

LACP Statistics

Use the following command to display Link Aggregation Control Protocol (LACP) statistics:

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

Command mode: All

Port EXT1:	

Valid LACPDUs received:	- 870
Valid Marker PDUs received:	- 0
Valid Marker Rsp PDUs received:	- 0
Unknown version/TLV type:	- 0
Illegal subtype received:	- 0
LACPDUs transmitted:	- 6031
Marker PDUs transmitted:	- 0
Marker Rsp PDUs transmitted:	- 0

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

Table 50. LACP Statistics

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

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 51. 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

Table 52. Layer 3 Statistics Commands

Command Syntax and Usage
<pre>show ip counters</pre> <p>Displays IP statistics. See page 74 for sample output.</p> <p>Command mode: All</p>
<pre>clear ip counters</pre> <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>
<pre>show ip dns counters</pre> <p>Displays Domain Name System (DNS) statistics. See page 76 for sample output.</p> <p>Command mode: All</p>
<pre>show ip tcp counters</pre> <p>Displays TCP statistics. See page 77 for sample output.</p> <p>Command mode: All</p>
<pre>show ip udp counters</pre> <p>Displays UDP statistics. See page 78 for sample output.</p> <p>Command mode: All</p>
<pre>clear ip dns counters</pre> <p>Clears Domain Name System (DNS) statistics.</p> <p>Command mode: All except User EXEC</p>
<pre>clear ip tcp counters</pre> <p>Clears Transmission Control Protocol (TCP) statistics.</p> <p>Command mode: All except User EXEC</p>
<pre>clear ip udp counters</pre> <p>Clears User Datagram Protocol (UDP) statistics.</p> <p>Command mode: All except User EXEC</p>

Table 52. Layer 3 Statistics Commands (continued)

Command Syntax and Usage	
clear ip counters	Clears IP statistics. Use this command with caution as it will delete all the IP statistics. Command mode: All
show layer3 counters	Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. Command mode: All

IPv4 Statistics

The following command displays IPv4 statistics:

```
show ip counters
```

Command mode: All

Use the following command to clear IPv4 statistics:

```
clear ip counters
```

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

Table 53. IP Statistics

Statistic	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.

Table 53. IP Statistics (continued)

Statistic	Description
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source-Route option processing was successful.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <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.

Table 53. IP Statistics (continued)

Statistic	Description
ipReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their <code>Don't Fragment</code> flag was set.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the <code>Time-To-Live (TTL)</code> 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 `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 54. 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 55. 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.
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.

Table 55. TCP Statistics (continued)

Statistic	Description
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurEstab	The total number of outstanding TCP sessions in the ESTABLISHED state.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

UDP Statistics

The following command displays UDP statistics:

```
show ip udp counters
```

Command mode: All

UDP statistics:			
udpInDatagrams:	54	udpOutDatagrams:	43
udpInErrors:	0	udpNoPorts:	1578077

Table 56. 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.

Management Processor Statistics

Table 57. Management Processor Statistics Commands

Command Syntax and Usage
<pre>show mp thread</pre> <p>Displays STEM thread statistics. This command is used by Technical Support personnel.</p> <p>Command mode: All</p>
<pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see page 81.</p> <p>Command mode: All</p>
<pre>show mp tcp-block</pre> <p>Displays all TCP control blocks that are in use. To view a sample output and a description of the statistics, see page 92.</p> <p>Command mode: All</p>
<pre>show mp udp-block</pre> <p>Displays all UDP control blocks that are in use. To view a sample output, see page 93.</p> <p>Command mode: All</p>
<pre>show processes cpu</pre> <p>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 93.</p> <p>Command mode: All</p>
<pre>show processes cpu history</pre> <p>Displays history of CPU utilization. To view a sample output, see page 96.</p> <p>Command mode: All</p>

Packet Statistics

Table 58. Packet Statistics Commands

Command Syntax and Usage
<pre>show mp packet counters</pre> <p>Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 81.</p> <p>Command mode: All</p>
<pre>clear mp packet logs</pre> <p>Clears all CPU packet statistics and logs.</p> <p>Command mode: All</p>

MP Packet Statistics

The following command displays MP packet statistics:

```
show mp packet counters
```

Command mode: All except User EXEC

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

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

Packet counters:	Received	Sent
-----	-----	----
Total packets:	109056	148761
Since bootup:	109056	148768
BPDUs:	6415	19214
Cisco packets:	0	0
ARP Requests:	15	10061
ARP Replies:	8545	14
LACP packets:	3414	3420
IPv4 packets:	60130	116101
ICMP Requests:	0	21
ICMP Replies:	21	0
IGMP packets:	0	0
PIM packets:	0	0
VRRP packets:	0	0
TCP packets:	60088	116113
FTP	0	0
HTTP	0	0
SSH	3	3
TACACS	0	0
TELNET	60095	116145
TCP other	0	0
UDP packets:	24	9
DHCP	0	0
NTP	0	0
RADIUS	0	0
SNMP	0	0
TFTP	0	0
UDP other	24	8
RIP packets:	0	1
OSPF packets:	0	0
BGP packets:	0	0
IPv6 packets:	0	0
LLDP PDUs:	3987	6876
FCoE FIP PDUs:	0	0
ECP PDUs:	0	0
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
```

Router(config)#

Problem 11:

page 239/612

output information have error, suggest use the form below.

Router(config)#show mp tcp-block

All TCP allocated control blocks:

```
145c1418: 0.0.0.0          0 <=>  
          0.0.0.0          179 listen  
1458cf48: 0:0:0:0:0:0:0:0      0 <=>  
          0:0:0:0:0:0:0:0      80 listen  
1458cdf8: 0.0.0.0          0 <=>  
          0.0.0.0          80 listen  
145d3610: 192.168.0.4        4130 <=>  
          10.38.5.151          23 established  
145a7658: 0:0:0:0:0:0:0:0      0 <=>  
          0:0:0:0:0:0:0:0      23 listen  
145a74d8: 0.0.0.0          0 <=>  
          0.0.0.0          23 listen
```

Table 59. 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.
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"> – IGMP – PIM – ICMP requests – ICMP replies
TCP packets	Total number of TCP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> – FTP – HTTP – SSH – TACACS+ – Telnet – Other
UDP packets	Total number of UDP packets received and sent. Includes the following packet types: <ul style="list-style-type: none"> – DHCP – NTP – RADIUS – SNMP – TFTP – Other
RIP packets	Total number of Routing Information Protocol packets received and sent.

Table 59. Packet Statistics (continued)

Statistics	Description
OSPF packets	Total number of Open Shortest Path First packets received and sent.
BGP packets	Total number of Border Gateway Protocol packets received and sent.
IPv6 packets	Total number of IPv6 packets received.
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 59. 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 60. Packet Statistics Log Options

Command Syntax and Usage
<pre>show mp packet log all</pre> <p>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 87.</p>
<pre>show mp packet log rx</pre> <p>Displays all packets logs received by the CPU.</p>
<pre>show mp packet log tx</pre> <p>Displays all packet logs sent from the CPU.</p>

Packet Log example

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

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

Each packet log entry includes the following information:

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

Packet Statistics Last Packet

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

Table 61. Last Packet Options

Command Syntax and Usage
<pre>show mp packet last both <I-1000></pre> <p>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 87.</p>
<pre>show mp packet last rx <I-1000></pre> <p>Displays a specified number of recent packet logs received by the CPU.</p>
<pre>show mp packet last tx <I-1000></pre> <p>Displays a specified number of recent packet logs sent from the CPU.</p>

Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

Table 62. Packet Statistics Dump Options

Command Syntax and Usage
<pre>show mp packet dump all</pre> <p>Displays all packet statistics and logs received by and sent from the CPU.</p>
<pre>show mp packet dump rx</pre> <p>Displays all packet statistics and logs received by the CPU.</p>
<pre>show mp packet dump tx</pre> <p>Displays all packet statistics and logs sent from the CPU.</p>

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 63](#).

Table 63. Packet Log Parsing Options

Command Syntax and Usage
<pre>show mp packet parse rx tx bpdu</pre> <p>Displays only BPDUs logged</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx cisco</pre> <p>Displays only Cisco packets (BPDU/CDP/UDLD) logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx lacp</pre> <p>Displays only LACP PDUs logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx fcoe</pre> <p>Displays only FCoE FIP PDUs logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx ipv4</pre> <p>Displays only IPv4 packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx tcp</pre> <p>Displays only TCP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx ftp</pre> <p>Displays only FTP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx http</pre> <p>Displays only HTTP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx ssh</pre> <p>Displays only SSH packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx tacacs</pre> <p>Displays only TACACS packets logged.</p> <p>Command mode: All</p>

Table 63. Packet Log Parsing Options (continued)

Command Syntax and Usage
<pre>show mp packet parse rx tx telnet</pre> <p>Displays only TELNET packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx tcpother</pre> <p>Displays only TCP other-port packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx udp</pre> <p>Displays only UDP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx ntp</pre> <p>Displays only NTP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx radius</pre> <p>Displays only RADIUS packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx snmp</pre> <p>Displays only SNMP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx tftp</pre> <p>Displays only TFTP packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx udpoth</pre> <p>Displays only UDP other-port packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx ipv6</pre> <p>Displays only IPv6 packets logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx lldp</pre> <p>Displays only LLDP PDUs logged.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx vlan <VLAN_number></pre> <p>Displays only logged packets with the specified VLAN.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx port <port_number></pre> <p>Displays only logged packets with the specified port.</p> <p>Command mode: All</p>

Table 63. Packet Log Parsing Options (continued)

Command Syntax and Usage
<pre>show mp packet parse rx tx mac <MAC_address></pre> <p>Displays only logged packets with the specified MAC address.</p> <p>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.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx other</pre> <p>Displays logs of all packets not explicitly selectable.</p> <p>Command mode: All</p>
<pre>show mp packet parse rx tx raw</pre> <p>Displays raw packet buffer in addition to headers.</p> <p>Command mode: All</p>

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 64. 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 except User EXEC

```

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 65. 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.

Table 65. CPU Statistics

Statistics	Description
Thread	The thread ID and name of the thread that caused the highest CPU use.
Time	The time when the highest CPU use was reached.

show processes cpu

Command mode: All

```

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

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

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

-----
Thread  Thread      Utilization      Status
  ID    Name         1sec      5sec      1Min      5Min
-----
  1     STEM        0.00%     0.00%     0.00%     0.00%     idle
  2     STP          0.00%     0.05%     0.10%     0.10%     idle
  3     MFDB         0.00%     0.00%     5.06%     5.22%     idle
  4     TND          0.00%     0.00%     0.00%     0.00%     idle
  5     CONS         0.00%     0.00%     0.00%     0.15%     suspended
  6     TNET         0.11%     0.58%     0.17%     0.27%     running
  7     TNET         0.00%     0.00%     0.00%     0.00%     idle
  8     TNET         0.00%     0.00%     0.00%     0.00%     idle
  9     TNET         0.00%     0.00%     0.00%     0.00%     idle
 10     LOG          0.00%     0.00%     0.00%     0.00%     idle
 11     TRAP         0.00%     0.00%     0.00%     0.00%     idle
 13     NTP          0.00%     0.00%     0.00%     0.00%     idle
 14     IP           0.04%     0.04%     0.06%     0.06%     idle
 17     IP           0.01%     0.08%     0.04%     0.04%     idle
 18     RIP          0.00%     0.00%     0.00%     0.00%     idle
 19     AGR          0.00%     0.00%     0.00%     0.00%     idle
 20     EPI          0.16%     0.27%     0.12%     0.10%     runnable
 22     PORT         0.00%     0.00%     0.00%     0.00%     idle
 24     BGP          0.18%     0.04%     0.00%     0.00%     idle
 32     SCAN         0.00%     0.00%     0.00%     0.00%     idle
 36     SNMP         0.00%     0.00%     0.00%     0.00%     idle
 37     SNMP         0.00%     0.00%     0.00%     0.00%     idle
 38     SNMP         0.00%     0.00%     0.00%     0.00%     idle
 40     SSHD         0.00%     0.00%     0.00%     0.00%     idle
...
120    VDPT         0.00%     0.00%     0.00%     0.00%     idle
124    HIST         0.00%     0.00%     0.00%     0.00%     runnable
128    NORM         0.00%     0.00%     0.00%     0.00%     idle
129    NORM         0.00%     0.00%     0.00%     0.00%     idle
130    DONE         0.00%     0.00%     0.00%     0.00%     idle
-----

```

Table 66. CPU Statistics

Statistics	Description
Thread ID	The thread ID number.
Thread Name	The name of the thread.
1sec	The percent of CPU use over 1 second.
5sec	The percent of CPU use over 5 seconds.
1Min	The percent of CPU use over 1 minute.
5Min	The percent of CPU use over 5 minutes.
Status	The status of the process.

CPU Statistics History

The following command 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 67. ACL Statistics Commands

Command Syntax and Usage
<pre>show access-control list <ACL number> counters</pre> <p>Displays the Access Control List Statistics for a specific ACL.</p> <p>Command mode: All</p>
<pre>show access-control list6 <ACL number> counters</pre> <p>Displays the IPv6 ACL statistics for a specific ACL.</p> <p>Command mode: All</p>
<pre>show access-control counters</pre> <p>Displays all ACL statistics.</p> <p>Command mode: All</p>
<pre>clear access-control list {<ACL number> all} counters</pre> <p>Clears ACL statistics.</p> <p>Command mode: Privileged EXEC</p>
<pre>clear access-control list6 {<ACL number> all}</pre> <p>Clears IPv6 ACL statistics.</p> <p>Command mode: Privileged EXEC</p>
<pre>show access-control meter <meter number> counters</pre> <p>Displays ACL meter statistics.</p> <p>Command mode: All</p>
<pre>clear access-control meter <meter number> counters</pre> <p>Clears ACL meter statistics.</p> <p>Command mode: Privileged EXEC</p>

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

Fibre Channel over Ethernet Statistics

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

```
show fcoe counters
```

Command mode: All

FCoE statistics:			
FCFAdded:	5	FCFRemoved:	1
FCOEAdded:	81	FCOERemoved:	24

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

Table 68. FCoE Statistics (/stats/fcoe)

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

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

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

```
clear fcoe counters
```

Command mode: 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 69. 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 69. 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> .
snmpInReadOnly	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.
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 <i>genErr</i> .

Table 69. SNMP Statistics (continued)

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

Table 69. SNMP Statistics (continued)

Statistic	Description
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of <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

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

The following command displays NTP statistics:

```
show ntp counters
```

Command mode: All

NTP statistics:	
Primary Server:	
Requests Sent:	17
Responses Received:	17
Updates:	1
Secondary Server:	
Requests Sent:	0
Responses Received:	0
Updates:	0
Last update based on response from primary/secondary server.	
Last update time: 18:04:16 Tue Jul 13, 2010	
Current system time: 18:55:49 Tue Jul 13, 2010	

Table 70. 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 70. NTP Statistics (continued)

Field	Description
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the following command was issued: <code>show ntp counters</code>

Statistics Dump

The following command dumps switch statistics:

```
show counters
```

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

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

Chapter 4. Configuration Commands

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

Table 71. General Configuration Commands

Command Syntax and Usage
<pre>show running-config</pre> <p>Dumps current configuration to a script file.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 202.</p>
<pre>show running-config diff</pre> <p>Displays running configuration changes that have been applied but not saved to flash memory.</p> <p>Command mode: Privileged EXEC</p>
<pre>copy running-config backup-config</pre> <p>Copy the current (running) configuration from switch memory to the backup-config partition.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 203.</p>
<pre>copy running-config startup-config</pre> <p>Copy the current (running) configuration from switch memory to the startup-config partition.</p> <p>Command mode: Privileged EXEC</p>
<pre>copy running-config {ftp tftp sftp} [extm-port mgt-port]</pre> <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: Privileged EXEC</p>
<pre>copy {ftp tftp sftp} running-config [extm-port mgt-port]</pre> <p>Restores current configuration from a FTP/TFTP/SFTP server. Select a management port, or press Enter to use the default (management) port.</p> <p>Command mode: Privileged EXEC</p> <p>For details, see page 204.</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 the following command:

```
Router# copy running-config startup-config
```

When you save configuration changes, the changes are saved to the *active* configuration block. For instructions on selecting the configuration to run at the next system reset, see [“Selecting a Configuration Block” on page 217](#).

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 72. System Configuration Commands

Command Syntax and Usage	
<pre>system date <yyy> <mm> <dd></pre>	<p>Prompts the user for the system date. The date retains its value when the switch is reset.</p> <p>Command mode: Global configuration</p>
<pre>system time <hh>:<mm>:<ss></pre>	<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>
<pre>system timezone</pre>	<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>
<pre>[no] system daylight</pre>	<p>Disables or enables 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.</p> <p>Command mode: Global configuration</p>
<pre>terminal-length <0-300></pre>	<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>
<pre>line console length <0-300></pre>	<p>Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is 28.</p> <p>Command mode: Global configuration</p>
<pre>no line console</pre>	<p>Sets <code>line console length</code> to the default value of 28.</p> <p>Command mode: Global configuration</p>
<pre>line vty length <0-300></pre>	<p>Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is 28.</p> <p>Command mode: Global configuration</p>

Table 72. System Configuration Commands (continued)

Command Syntax and Usage	
<code>no line vty</code>	<p>Sets line vty length to the default value of 28.</p> <p>Command mode: Global configuration</p>
<code>system idle <0-60></code>	<p>Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle.</p> <p>Command mode: Global configuration</p>
<code>system linkscan {fast normal slow}</code>	<p>Configures the link scan interval used to poll the status of ports.</p> <p>Command mode: Global configuration</p>
<code>system notice <maximum 1024 character multi-line login notice> <'.' to end></code>	<p>Displays 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>
<code>[no] banner <1-80 characters></code>	<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>
<code>[no] hostname <character string></code>	<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>
<code>[no] system dhcp [extm mgt]</code>	<p>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 <code>enabled</code>.</p> <p>Command mode: Global configuration</p>
<code>[no] system reset-control</code>	<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>

Table 72. System Configuration Commands (continued)

Command Syntax and Usage
<code>[no] system packet-logging</code> Enables or disables logging of packets that come to the CPU. The default setting is enabled. Command mode: Global configuration
<code>show system</code> Displays the current system parameters. Command mode: All

System Error Disable and Recovery Configuration

The Error Disable and Recovery feature allows the switch to automatically disable a port if an error condition is detected on the port. The port remains in the error-disabled state until it is re-enabled manually, or re-enabled automatically by the switch after a timeout period has elapsed. The error-disabled state of a port does not persist across a system reboot.

Table 73. Error Disable Configuration Commands

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

System Host Log Configuration

Table 74. Host Log Configuration Commands

Command Syntax and Usage	
[no] logging host <1-2> address <IP address> [extm-port mgt-port]	Sets the IPv4 address of the first or second syslog host. Command mode: Global configuration
[no] logging host <1-2> address6 <IP address> [extm-port mgt-port]	Sets the IPv6 address of the first or second syslog host. Command mode: Global configuration
logging host <1-2> severity <0-7>	This option sets the severity level of the first or second syslog host displayed. The default is 7, which means log all severity levels. Command mode: Global configuration
logging host <1-2> facility <0-7>	This option sets the facility level of the first or second syslog host displayed. The default is 0. Command mode: Global configuration
logging source-interface <1-5>	Sets the loopback interface number for syslogs. Command mode: Global configuration
logging console	Enables delivering syslog messages to the console. It is enabled by default. Command mode: Global configuration
no logging console	Disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default. Command mode: Global configuration

Table 74. Host Log Configuration Commands

Command Syntax and Usage	
[no] logging synchronous [level <0-7> all]	<p>Enables or disables synchronous logging for unsolicited messages. When enabled, if unsolicited messages occur while solicited output display is in progress, the unsolicited messages are buffered and then output separately from the solicited messages. The buffer can store up to 20 unsolicited messages, after which unsolicited messages are discarded. When disabled, unsolicited and solicited messages are logged together.</p> <p>The <code>level</code> parameter sets a minimum severity level (lower or equal numeric values) for unsolicited messages to be displayed asynchronously; <code>all</code> displays all unsolicited messages asynchronously, regardless of severity level. The default setting is 2.</p> <p>Command mode: Global configuration</p>
logging console severity <0-7>	<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. The default is 7, which means log all severity levels.</p> <p>Command mode: Global configuration</p>
no logging console severity	<p>Disables delivering syslog messages to the console based on severity.</p> <p>Command mode: Global configuration</p>
[no] logging buffer severity <0-7>	<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>Command mode: Global configuration</p>
[no] logging log [<feature>]	<p>Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as <code>vlan</code>s, <code>stg</code>, or <code>ssh</code>), or enable/disable syslog on all available features.</p> <p>Command mode: Global configuration</p>
show logging [severity <severity level>] [reverse]	<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 22.</p> <p>The <code>reverse</code> 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 10Gb System Interconnect Module, these commands enable Secure Shell access from any SSH client.

Table 75. SSH Server Configuration Commands

Command Syntax and Usage	
<code>ssh scp-password</code>	Set the administration password for SCP access. Command mode: Global configuration
<code>ssh generate-host-key</code>	Generate the RSA host key. Command mode: Global configuration
<code>ssh port <TCP port number></code>	Sets the SSH server port number. Command mode: Global configuration
<code>ssh scp-enable</code>	Enables the SCP apply and save. Command mode: Global configuration
<code>no ssh scp-enable</code>	Disables the SCP apply and save. Command mode: Global configuration
<code>ssh enable</code>	Enables the SSH server. Command mode: Global configuration
<code>no ssh enable</code>	Disables the SSH server. Command mode: Global configuration
<code>show ssh</code>	Displays the current SSH server configuration. Command mode: All

RADIUS Server Configuration

Table 76. RADIUS Server Configuration Commands

Command Syntax and Usage	
[no] radius-server primary-host <IP address>	Sets the primary RADIUS server address. Command mode: Global configuration
[no] radius-server secondary-host <IP address>	Sets the secondary RADIUS server address. Command mode: Global configuration
radius-server primary-host <IP address> key <1-32 characters>	This is the primary shared secret between the switch and the RADIUS server(s). Command mode: Global configuration
radius-server secondary-host <IP address> key <1-32 characters>	This is the secondary shared secret between the switch and the RADIUS server(s). Command mode: Global configuration
[default] radius-server port <UDP port number>	Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645. Command mode: Global configuration
radius-server retransmit <1-3>	Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests. Command mode: Global configuration
radius-server timeout <1-10>	Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds. Command mode: Global configuration
[no] radius-server backdoor	Enables or disables the RADIUS backdoor for Telnet/SSH/HTTP/HTTPS. The default value is disabled. To obtain the RADIUS backdoor password for your switch, contact your Service and Support line. Command mode: Global configuration
radius-server enable	Enables the RADIUS server. Command mode: Global configuration

Table 76. RADIUS Server Configuration Commands

Command Syntax and Usage
<code>no radius-server enable</code> Disables the RADIUS server. Command mode: Global configuration
<code>show radius-server</code> Displays the current RADIUS server parameters. Command mode: All

TACACS+ Server Configuration

TACACS (Terminal Access Controller Access Control system) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS is not an encryption protocol, and therefore less secure than TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols. Both TACACS and TACACS+ are described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports de-coupled authentication, authorization, and accounting.

Table 77. TACACS+ Server Configuration Commands

Command Syntax and Usage
<pre>[no] tacacs primary-host <IP address></pre> <p>Defines the primary TACACS+ server address.</p> <p>Command mode: Global configuration</p>
<pre>[no] tacacs secondary-host <IP address></pre> <p>Defines the secondary TACACS+ server address.</p> <p>Command mode: Global configuration</p>
<pre>[no] tacacs primary-host <IP address> key <1-32 characters></pre> <p>This is the primary shared secret between the switch and the TACACS+ server(s).</p> <p>Command mode: Global configuration</p>
<pre>[no] tacacs secondary-host <IP address> key <1-32 characters></pre> <p>This is the secondary shared secret between the switch and the TACACS+ server(s).</p> <p>Command mode: Global configuration</p>
<pre>[default] tacacs port <TCP port number></pre> <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>
<pre>tacacs retransmit <1-3></pre> <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>

Table 77. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage	
<code>tacacs attempts <1-10></code>	<p>Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.</p> <p>Command mode: Global configuration</p>
<code>tacacs timeout <4-15></code>	<p>Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p>Command mode: Global configuration</p>
<code>[no] tacacs user-mapping {<0-15> user oper admin}</code>	<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>
<code>[no] tacacs backdoor</code>	<p>Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.</p> <p>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.</p> <p>The default setting is <code>disabled</code>.</p> <p>To obtain the TACACS+ backdoor password for your SI4093, contact your Service and Support line.</p> <p>Command mode: Global configuration</p>
<code>[no] tacacs secure-backdoor</code>	<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>
<code>[no] tacacs privilege-mapping</code>	<p>Enables or disables TACACS+ privilege-level mapping.</p> <p>The default value is <code>disabled</code>.</p> <p>Command mode: Global configuration</p>

Table 77. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage	
[no] tacacs-server password-change	<p>Enables or disables TACACS+ password change. The default value is disabled.</p> <p>Command mode: Global configuration</p>
primary-password	<p>Configures the password for the primary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p>
secondary-password	<p>Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.</p> <p>Command mode: Global configuration</p>
[no] tacacs-server command-authorization	<p>Enables or disables TACACS+ command authorization.</p> <p>Command mode: Global configuration</p>
[no] tacacs-server command-logging	<p>Enables or disables TACACS+ command logging.</p> <p>Command mode: Global configuration</p>
[no] tacacs-server directed-request [restricted no-truncate]	<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"> – Restricted: Only the username is sent to the specified TACACS+ server. – No-truncate: The entire login string is sent to the TACACS+ server. <p>Command mode: Global configuration</p>
[no] tacacs-server enable	<p>Enables or disables the TACACS+ server. By default, the server is disabled.</p> <p>Command mode: Global configuration</p>
[no] tacacs-server accounting-enable	<p>Enables or disables TACACS+ accounting.</p> <p>Command mode: Global configuration</p>
show tacacs-server	<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 78. LDAP Server Configuration Commands

Command Syntax and Usage	
[no] ldap-server primary-host <IP address>	<p>Sets the primary LDAP server address.</p> <p>Command mode: Global configuration</p>
[no] ldap-server secondary-host <IP address>	<p>Sets the secondary LDAP server address.</p> <p>Command mode: Global configuration</p>
[default] ldap-server port <UDP port number>	<p>Enter the number of the UDP port to be configured, between 1 - 65000. The default is 389.</p> <p>Command mode: Global configuration</p>
ldap-server retransmit <1-3>	<p>Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.</p> <p>Command mode: Global configuration</p>
ldap-server timeout <4-15>	<p>Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.</p> <p>Command mode: Global configuration</p>
ldap-server domain [<1-128 characters> none]	<p>Sets the domain name for the LDAP server. Enter the full path for your organization. For example:</p> <p>ou=people, dc=mydomain, dc=com</p> <p>Command mode: Global configuration</p>
[no] ldap-server backdoor	<p>Enables or disables the LDAP back door for Telnet, SSH/SCP, or HTTP/HTTPS. The default setting is disabled.</p> <p>To obtain the LDAP back door password for your SI4093, contact your Service and Support line.</p> <p>Command mode: Global configuration</p>

Table 78. LDAP Server Configuration Commands (continued)

Command Syntax and Usage
<code>ldap-server enable</code> Enables the LDAP server. Command mode: Global configuration
<code>no ldap-server enable</code> Disables the LDAP server. Command mode: Global configuration
<code>show ldap-server</code> Displays the current LDAP server parameters. Command mode: All

NTP Server Configuration

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

Table 79. NTP Server Configuration Commands

Command Syntax and Usage	
<pre>[no] ntp primary-server <IP address>[extm-port mgt-port]</pre>	<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"> – internal management port (mgt) – external management port (extm) <p>Command mode: Global configuration</p>
<pre>[no] ntp secondary-server <IP address>[extm-port mgt-port]</pre>	<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"> – internal management port (mgt) – external management port (extm) <p>Command mode: Global configuration</p>
<pre>[no] ntp ipv6 primary-server <IPv6 address>[extm-port mgt-port]</pre>	<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"> – internal management port (mgt) – external management port (extm) <p>Note: To delete the IPv6 primary server, use the following command: no ntp primary-server <IP address></p> <p>Command mode: Global configuration</p>
<pre>[no] ntp ipv6 secondary-server <IPv6 address>[extm-port mgt-port]</pre>	<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"> – internal management port (mgt) – external management port (extm) <p>Note: To delete the IPv6 secondary server, use the following command: no ntp secondary-server <IP address></p> <p>Command mode: Global configuration</p>
<pre>ntp interval <5-44640></pre>	<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>

Table 79. NTP Server Configuration Commands

Command Syntax and Usage
<pre>[no] ntp authenticate</pre> <p>Enables or disables NTP authentication. The default setting is disabled. When authentication is enabled, the switch transmits NTP packets with the MAC address appended.</p> <p>Command mode: Global configuration</p>
<pre>ntp primary-key <1-65534></pre> <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>
<pre>ntp secondary-key <1-65534></pre> <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>
<pre>ntp trusted-key <1-65534> 0</pre> <p>Adds 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>
<pre>ntp enable</pre> <p>Enables the NTP synchronization service.</p> <p>Command mode: Global configuration</p>
<pre>no ntp enable</pre> <p>Disables the NTP synchronization service.</p> <p>Command mode: Global configuration</p>
<pre>show ntp</pre> <p>Displays the current NTP service settings.</p> <p>Command mode: All</p>

NTP MD5 Key Commands

Table 80. NTP MD5 KEY Configuration Options

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

System SNMP Configuration

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

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

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

SNMP parameters that can be modified include:

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

Table 81. System SNMP Commands

Command Syntax and Usage
<pre>snmp-server name <1-64 characters></pre> <p>Configures the name for the system. The name can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server location <1-64 characters></pre> <p>Configures the name of the system location. The location can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server contact <1-64 characters></pre> <p>Configures the name of the system contact. The contact can have a maximum of 64 characters.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server read-community <1-32 characters></pre> <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. The default read community string is <i>public</i>.</p> <p>Command mode: Global configuration</p>

Table 81. System SNMP Commands

Command Syntax and Usage	
<code>snmp-server write-community <1-32 characters></code>	<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. The default write community string is <i>private</i>.</p> <p>Command mode: Global configuration</p>
<code>[no] snmp-server read-community-additional <1-32 characters></code>	<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>
<code>[no] snmp-server write-community-additional <1-32 characters></code>	<p>Adds or removes an additional SNMP write community string. Up to 7 additional write community strings are supported.</p> <p>Command mode: Global configuration</p>
<code>snmp-server trap-source {<interface number>}</code>	<p>Configures the source interface for SNMP traps.</p> <p>To send traps through the management ports, specify interface 4.</p> <p>Command mode: Global configuration</p>
<code>snmp-server host <trap host IP address> <trap host community string></code>	<p>Adds a trap host server.</p> <p>Command mode: Global configuration</p>
<code>no snmp-server host <trap host IP address></code>	<p>Removes the trap host server.</p> <p>Command mode: Global configuration</p>
<code>snmp-server timeout <1-30></code>	<p>Sets the timeout value for the SNMP state machine, in minutes.</p> <p>Command mode: Global configuration</p>
<code>[no] snmp-server authentication-trap</code>	<p>Enables or disables the use of the system authentication trap facility. The default setting is disabled.</p> <p>Command mode: Global configuration</p>
<code>[no] snmp-server link-trap</code>	<p>Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.</p> <p>Command mode: Global configuration</p>
<code>show snmp-server</code>	<p>Displays the current SNMP configuration.</p> <p>Command mode: All</p>

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 82. SNMPv3 Configuration Commands

Command Syntax and Usage
<pre>snmp-server user <I-16></pre> <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.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 129.</p>
<pre>snmp-server view <I-128></pre> <p>This command allows you to create different MIB views.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 130.</p>
<pre>snmp-server access <I-32></pre> <p>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.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 131.</p>
<pre>snmp-server group <I-16></pre> <p>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.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 132.</p>
<pre>snmp-server community <I-16></pre> <p>The community table contains objects for mapping community strings and version-independent SNMP message parameters.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 133.</p>

Table 82. SNMPv3 Configuration Commands (continued)

<pre>snmp-server target-address <I-16></pre> <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.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 134.</p>
<pre>snmp-server target-parameters <I-16></pre> <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.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 135.</p>
<pre>snmp-server notify <I-16></pre> <p>A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 136.</p>
<pre>snmp-server version {v1v2v3 v3only}</pre> <p>This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. The default value is v1v2v3.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3</pre> <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 83. User Security Model Configuration Commands

Command Syntax and Usage	
<pre>snmp-server user <1-16> name <1-32 characters></pre>	<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>
<pre>snmp-server user <1-16> authentication-protocol {md5 sha none} authentication-password <password value></pre>	<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, or none. The default algorithm is none.</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>
<pre>snmp-server user <1-16> privacy-protocol {des none} privacy-password <password value></pre>	<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 <i>des</i> (CBC-DES Symmetric Encryption Protocol) or <i>none</i>. If you specify <i>des</i> as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select <i>none</i> 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>
<pre>no snmp-server user <1-16></pre>	<p>Deletes the USM user entries.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 user <1-16></pre>	<p>Displays the USM user entries.</p> <p>Command mode: All</p>

SNMPv3 View Configuration

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

Table 84. SNMPv3 View Configuration Commands

Command Syntax and Usage	
<code>snmp-server view <1-128> name <1-32 characters></code>	This command defines the name for a family of view subtrees. Command mode: Global configuration
<code>snmp-server view <1-128> tree <1-64 characters></code>	This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. Command mode: Global configuration
<code>[no] snmp-server view <1-128> mask <1-32 characters></code>	This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. Command mode: Global configuration
<code>snmp-server view <1-128> type {included excluded}</code>	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
<code>no snmp-server view <1-128></code>	Deletes the <code>vacmViewTreeFamily</code> group entry. Command mode: Global configuration
<code>show snmp-server v3 view <1-128></code>	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 85. View-based Access Control Model Commands

Command Syntax and Usage
<pre>snmp-server access <1-32> name <1-32 characters></pre> <p>Defines the name of the group.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server access <1-32> prefix <1-32 characters></pre> <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 contextName.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server access <1-32> security {usm snmpv1 snmpv2}</pre> <p>Allows you to select the security model to be used.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server access <1-32> level {noAuthNoPriv authNoPriv authPriv}</pre> <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>
<pre>snmp-server access <1-32> match {exact prefix}</pre> <p>If the value is set to <code>exact</code>, then all the rows whose contextName 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 contextName exactly match the prefix are selected.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server access <1-32> read-view <1-32 characters></pre> <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 85. View-based Access Control Model Commands (continued)

Command Syntax and Usage
<pre>snmp-server access <1-32> write-view <1-32 characters></pre> <p>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.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server access <1-32> notify-view <1-32 characters></pre> <p>Defines a notify view name that allows you notify access to the MIB view.</p> <p>Command mode: Global configuration</p>
<pre>no snmp-server access <1-32></pre> <p>Deletes the View-based Access Control entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 access <1-32></pre> <p>Displays the View-based Access Control configuration.</p> <p>Command mode: All</p>

SNMPv3 Group Configuration

Table 86. SNMPv3 Group Configuration Commands

Command Syntax and Usage
<pre>snmp-server group <1-16> security {usm snmpv1 snmpv2}</pre> <p>Defines the security model.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server group <1-16> user-name <1-32 characters></pre> <p>Sets the user name as defined in the following command on page 129: <pre>snmp-server user <1-16> name <1-32 characters></pre></p> <p>Command mode: Global configuration</p>
<pre>snmp-server group <1-16> group-name <1-32 characters></pre> <p>The name for the access group as defined in the following command: <pre>snmp-server access <1-32> name <1-32 characters></pre> on page 129.</p> <p>Command mode: Global configuration</p>
<pre>no snmp-server group <1-16></pre> <p>Deletes the vacmSecurityToGroup entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 group <1-16></pre> <p>Displays the current vacmSecurityToGroup configuration.</p> <p>Command mode: All</p>

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 87. SNMPv3 Community Table Configuration Commands

Command Syntax and Usage
<pre>snmp-server community <1-16> index <1-32 characters></pre> <p>Allows you to configure the unique index value of a row in this table.</p> <p>Command string: Global configuration</p>
<pre>snmp-server community <1-16> name <1-32 characters></pre> <p>Defines the user name as defined in the following command on page 129: <pre>snmp-server user <1-16> name <1-32 characters></pre></p> <p>Command string: Global configuration</p>
<pre>snmp-server community <1-16> user-name <1-32 characters></pre> <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>
<pre>snmp-server community <1-16> tag <1-255 characters></pre> <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>
<pre>no snmp-server community <1-16></pre> <p>Deletes the community table entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 community <1-16></pre> <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 88. Target Address Table Configuration Commands

Command Syntax and Usage
<pre>snmp-server target-address <1-16> address <IP address> name <1-32 characters></pre> <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>
<pre>snmp-server target-address <1-16> name <1-32 characters> address <transport IP address></pre> <p>Configures a transport IPv4 address that can be used in the generation of SNMP traps.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server target-address <1-16> port <port number></pre> <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>
<pre>snmp-server target-address <1-16> taglist <1-255 characters></pre> <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>
<pre>snmp-server target-address <1-16> parameters-name <1-32 characters></pre> <p>Defines the name as defined in the following command on page 135: <pre>snmp-server target-parameters <1-16> name <1-32 characters></pre></p> <p>Command mode: Global configuration</p>
<pre>no snmp-server target-address <1-16></pre> <p>Deletes the Target Address Table entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 target-address <1-16></pre> <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 89. Target Parameters Table Configuration Commands

Command Syntax and Usage
<pre>snmp-server target-parameters <I-16> name <I-32 characters></pre> <p>Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server target-parameters <I-16> message {snmpv1 snmpv2c snmpv3}</pre> <p>Allows you to configure the message processing model that is used to generate SNMP messages.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server target-parameters <I-16> security {usm snmpv1 snmpv2}</pre> <p>Allows you to select the security model to be used when generating the SNMP messages.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server target-parameters <I-16> user-name <I-32 characters></pre> <p>Defines the name that identifies the user in the USM table (page 129) on whose behalf the SNMP messages are generated using this entry.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server target-parameters <I-16> level {noAuthNoPriv authNoPriv authPriv}</pre> <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>
<pre>no snmp-server target-parameters <I-16></pre> <p>Deletes the <code>targetParamsTable</code> entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 target-parameters <I-16></pre> <p>Displays the current <code>targetParamsTable</code> configuration.</p> <p>Command mode: All</p>

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 90. Notify Table Commands

Command Syntax and Usage
<pre>snmp-server notify <1-16> name <1-32 characters></pre> <p>Defines a locally arbitrary, but unique, identifier associated with this SNMP notify entry.</p> <p>Command mode: Global configuration</p>
<pre>snmp-server notify <1-16> tag <1-255 characters></pre> <p>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 <code>snmpTargetAddrTable</code>, that matches the value of this tag, is selected.</p> <p>Command mode: Global configuration</p>
<pre>no snmp-server notify <1-16></pre> <p>Deletes the notify table entry.</p> <p>Command mode: Global configuration</p>
<pre>show snmp-server v3 notify <1-16></pre> <p>Displays the current notify table configuration.</p> <p>Command mode: All</p>

System Access Configuration

The following table describes system access configuration commands.

Table 91. System Access Configuration Commands

Command Syntax and Usage
<pre>access user user-password</pre> <p>Sets the user (<code>user</code>) 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>
<pre>access user operator-password</pre> <p>Sets the operator (<code>oper</code>) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports.</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 operator account, set the password to null (no password). The default setting is disabled (no password).</p> <p>Command Mode: Global configuration</p>
<pre>access user administrator-password</pre> <p>Sets the administrator (<code>admin</code>) 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.</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>Access includes “oper” functions.</p> <p>Note: You cannot disable the administrator password.</p> <p>Command Mode: Global configuration</p>
<pre>[no] access snmp {read-only read-write}</pre> <p>Disables or provides read-only/write-read SNMP access.</p> <p>Command mode: Global configuration</p>
<pre>[no] access telnet enable</pre> <p>Enables or disables Telnet access. This command is enabled by default.</p> <p>Command mode: Global configuration</p>
<pre>[default] access telnet port [<1-65535>]</pre> <p>Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port.</p> <p>Command mode: Global configuration</p>

Table 91. System Access Configuration Commands (continued)

Command Syntax and Usage
<pre>[default] access tftp-port [<1-65535>]</pre> <p>Sets the TFTP port for the switch. The default is port 69.</p> <p>Command mode: Global configuration</p>
<pre>show access</pre> <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.

Table 92. Management Network Configuration Commands

Command Syntax and Usage
<pre>access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length></pre> <p>Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the IBM Networking OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation.</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>
<pre>no access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length></pre> <p>Removes a defined network, which consists of a management network address and a management network mask address.</p> <p>Command mode: Global configuration</p>
<pre>access management-network <mgmt network IPv4 or IPv6 address> <mgmt network mask or prefix length> {snmp-ro snmp-rw}</pre> <p>Adds a defined 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>
<pre>no access management-network {snmp-ro snmp-rw}</pre> <p>Clears the SNMP read-only or SNMP read/write access control list for management purposes.</p> <p>Command mode: Global configuration</p>

Table 92. Management Network Configuration Commands

Command Syntax and Usage
<pre>show access management-network</pre> <p>Displays the current management network configuration and SNMP access management IP list.</p> <p>Command mode: All</p>
<pre>clear access management-network</pre> <p>Removes all defined management networks.</p> <p>Command mode: All except User EXEC</p>

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 93. User Access Control Configuration Commands

Command Syntax and Usage
<pre>access user <1-10></pre> <p>Configures the User ID.</p> <p>Command mode: Global configuration</p>
<pre>access user eject {<user name> <session ID>}</pre> <p>Ejects the specified user from the SI4093.</p> <p>Command mode: Global configuration</p>
<pre>clear line <1-12></pre> <p>Ejects the user with the corresponding session ID from the SI4093.</p> <p>Command mode: Privileged EXEC</p>
<pre>access user user-password <1-128 characters></pre> <p>Sets the user (<code>user</code>) 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>
<pre>access user operator-password <1-128 characters></pre> <p>Sets the operator (<code>oper</code>) 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>
<pre>access user administrator-password <1-128 characters></pre> <p>Sets the administrator (<code>admin</code>) 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.</p> <p>Access includes “oper” functions.</p> <p>Command mode: Global configuration</p>
<pre>show access user</pre> <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 94. User ID Configuration Commands

Command Syntax and Usage
<pre>access user <1-10> level {user operator administrator}</pre> <p>Sets the Class-of-Service to define the user's authority level. IBM Networking OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.</p> <p>Command mode: Global configuration</p>
<pre>access user <1-10> name <1-8 characters></pre> <p>Defines the user name of maximum eight characters.</p> <p>Command mode: Global configuration</p>
<pre>access user <1-10> password</pre> <p>Sets the user (<code>user</code>) password. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password.</p> <p>Command mode: Global configuration</p>
<pre>access user <1-10> enable</pre> <p>Enables the user ID.</p> <p>Command mode: Global configuration</p>
<pre>no access user <1-10> enable</pre> <p>Disables the user ID.</p> <p>Command mode: Global configuration</p>
<pre>no access user <1-10></pre> <p>Deletes the user ID.</p> <p>Command mode: Global configuration</p>
<pre>show access user</pre> <p>Displays the current user ID configuration.</p> <p>Command mode: All</p>

Strong Password Configuration

The following table describes strong password configuration commands.

Table 95. Strong Password Configuration Commands

Command Syntax and Usage
<pre>access user strong-password enable</pre> <p>Enables Strong Password requirement. Command mode: Global configuration</p>
<pre>no access user strong-password enable</pre> <p>Disables Strong Password requirement. Command mode: Global configuration</p>
<pre>access user strong-password expiry <1-365></pre> <p>Configures the number of days allowed before the password must be changed. The default value is 60 days. Command mode: Global configuration</p>
<pre>access user strong-password warning <1-365></pre> <p>Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days. Command mode: Global configuration</p>
<pre>access user strong-password faillog <1-255></pre> <p>Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts. Command mode: Global configuration</p>
<pre>[no] access user strong-password lockout</pre> <p>Enables or disables account lockout after a specified number of failed login attempts. Default setting is disabled. Command mode: Global configuration</p>
<pre>access user strong-password faillock <1-10></pre> <p>Configures the number of failed login attempts that trigger the account lockout. Default value is 6. Command mode: Global configuration</p>
<pre>access user strong-password clear local user {lockout fail-attempts} {<username> all}</pre> <p>Enables locked out accounts or resets failed login counters for all users or for a specific user. Command mode: Global configuration</p>
<pre>show access user strong-password</pre> <p>Displays the current Strong Password configuration. 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 96. Custom DST Configuration Commands

Command Syntax and Usage
<pre>system custom-dst start-rule <WDDMMhh></pre> <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) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) 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>
<pre>system custom-dst end-rule <WDDMMhh></pre> <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) D = day of the week (01-07, where 01 is Monday) MM = month (1-12) 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>
<pre>system custom-dst enable</pre> <p>Enables the Custom Daylight Saving Time settings.</p> <p>Command mode: Global configuration</p>
<pre>no system custom-dst enable</pre> <p>Disables the Custom Daylight Savings Time settings.</p> <p>Command mode: Global configuration</p>
<pre>show custom-dst</pre> <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 (INT_x) and (EXT_x). If you are configuring management ports (MGT1), see [“Management Port Configuration” on page 151](#).

Table 97. Port Configuration Commands

Command Syntax and Usage	
interface port <port alias or number>	Enter Interface port mode. Command mode: Global configuration
pvid <VLAN number>	Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports. Command mode: Interface port
name <1-64 characters>	Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default is set to None. Command mode: Interface port
unicast-bandwidth <10-100>	Configures the allocated bandwidth percentage for unicast traffic on the port. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. Command mode: Interface port
unicast-bandwidth global <10-100>	Configures the allocated bandwidth percentage for unicast traffic on the egress ports. The remaining bandwidth is automatically allocated to multicast traffic. The default value is 50. This applies to all ports. Command mode: Interface port
[no] tagging	Disables or enables VLAN tagging for this port. The default setting is disabled for external ports (EXT _x) and enabled for internal server ports (INT _x). Command mode: Interface port
[no] tag-pvid	Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is disabled for internal server ports (INT _x) and external ports (EXT _x), and enabled for management (MGT _x) ports. Command mode: Interface port

Table 97. Port Configuration Commands (continued)

Command Syntax and Usage	
[no] tagpvid-ingress	<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. The default setting is disabled.</p> <p>Command mode: Interface port/Interface portchannel</p>
[no] flood-blocking	<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>
[no] mac-address-table mac-notification	<p>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.</p> <p>Command mode: Interface port/Interface portchannel</p>
[no] learning	<p>Enables or disables FDB learning on the port.</p> <p>Command mode: Interface port</p>
port-channel min-links <1-32>	<p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the down state.</p> <p>Command mode: Interface port</p>
[no] broadcast-threshold <0-262143>	<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>
[no] multicast-threshold <0-262143>	<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>
[no] dest-lookup-threshold <0-262143>	<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>
no shutdown	<p>Enables the port.</p> <p>Command mode: Interface port</p>

Table 97. Port Configuration Commands (continued)

Command Syntax and Usage
<pre>shutdown</pre> <p>Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to “Temporarily Disabling a Port” on page 147.)</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number></pre> <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 98. Port Error Disable Commands

Command Syntax and Usage
<pre>errdisable recovery</pre> <p>Enables automatic error-recovery for the port. The default setting is <code>enabled</code>.</p> <p>Note: Error-recovery must be enabled globally before port-level commands become active.</p> <p>Command mode: Interface port</p>
<pre>no errdisable recovery</pre> <p>Enables automatic error-recovery for the port.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number> errdisable</pre> <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 99. Port Link Configuration Commands

Command Syntax and Usage
<pre>speed {10 100 1000 10000 auto}</pre> <p>Sets the link speed. Some options are not valid on all ports. The choices include:</p> <ul style="list-style-type: none"> – 1000 Mbps – 10000 Mps – any (auto negotiate port speed) <p>Command mode: Interface port</p>
<pre>duplex {full half any}</pre> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> – Any negotiation (default) – Half-duplex – Full-duplex <p>Command mode: Interface port</p>
<pre>flowcontrol {receive send} [on off]</pre> <p>Sets the flow control. The choices include:</p> <ul style="list-style-type: none"> – Receive flow control – Transmit flow control – No flow control <p>Note: For external ports (EXTx) the default setting is no flow control, and for internal ports (INTx) the default setting is both receive and transmit.</p> <p>Command mode: Interface port</p>
<pre>[no] auto</pre> <p>Turns auto-negotiation on or off.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number></pre> <p>Displays current port parameters.</p> <p>Command mode: All</p>

Temporarily Disabling a Port

To temporarily disable a port without changing its stored configuration attributes, enter the following command at any prompt:

```
Router# interface port <port alias or number> shutdown
```

Because this configuration sets a temporary state for the port, you do not need to use a save operation. The port state will revert to its original configuration when the SI4093 10Gb System Interconnect Module is reset. See the [“Operations Commands” on page 205](#) for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 100. Port UDLD Configuration Commands

Command Syntax and Usage
<pre>[no] udld</pre> <p>Enables or disables UDLD on the port.</p> <p>Command mode: Interface port</p>
<pre>[no] udld aggressive</pre> <p>Configures the UDLD mode for the selected port, as follows:</p> <ul style="list-style-type: none"> – Normal: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the “no” form to select normal operation. – Aggressive: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. <p>Command mode: Interface port</p>
<pre>show interface port <port number> udld</pre> <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 101. Port OAM Configuration Commands

Command Syntax and Usage
<pre>oam {active passive}</pre> <p>Configures the OAM discovery mode, as follows:</p> <ul style="list-style-type: none"> – Active: This port link initiates OAM discovery. – 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>
<pre>no oam {active passive}</pre> <p>Disables OAM discovery on the port.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port number> oam</pre> <p>Displays current port OAM parameters.</p> <p>Command mode: All</p>

Port ACL Configuration

The following table describes port ACL configuration commands

Table 102. Port ACL/QoS Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <ACL number></pre> <p>Adds or removes the specified ACL. You can add multiple ACLs to a port.</p> <p>Command mode: Interface port</p>
<pre>[no] access-control list6 <ACL number></pre> <p>Adds or removes the specified IPv6 ACL. You can add multiple ACLs to a port.</p> <p>Command mode: Interface port</p>
<pre>[no] access-control group <ACL group number></pre> <p>Adds or removes the specified ACL group. You can add multiple ACL groups to a port.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number> access-control</pre> <p>Displays current ACL QoS parameters.</p> <p>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 153](#).

Table 103. Port WRED Options

Command Syntax and Usage
<pre>[no] random-detect ecn enable</pre> <p>Enables or disables Explicit Congestion Notification (ECN). When ECN is on, the switch marks the ECN bit of the packet (if applicable) instead of dropping the packet. ECN-aware devices are notified of the congestion and those devices can take corrective actions.</p> <p>Note: ECN functions only on TCP traffic.</p> <p>Command mode: Interface port</p>
<pre>random-detect enable</pre> <p>Turns on Random Detection and avoidance.</p> <p>Command mode: Interface port</p>
<pre>no random-detect enable</pre> <p>Turns off Random Detection and avoidance.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number> random-detect</pre> <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 104. Port WRED Transmit Queue Options

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

Table 104. Port WRED Transmit Queue Options

Command Syntax and Usage
<pre>random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p>Command mode: Interface port</p>
<pre>no random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p>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, the values for speed, duplex, and flow control are fixed, and cannot be configured.

Table 105. Management Port Configuration Commands

Command Syntax and Usage
<pre>speed {10 100 1000 auto}</pre> <p>Sets the link speed. The choices include:</p> <ul style="list-style-type: none"> – 10 Mbps – 100 Mbps – 1000 Mbps – Auto — for auto negotiation <p>Command mode: Interface port</p>
<pre>duplex {full half any}</pre> <p>Sets the operating mode. The choices include:</p> <ul style="list-style-type: none"> – Full-duplex – Half-duplex – Any — for auto negotiation (default) <p>Command mode: Interface port</p>
<pre>[no] flowcontrol {receive send both}</pre> <p>Sets the flow control. The choices include:</p> <ul style="list-style-type: none"> – Receive flow control – Transmit flow control – Both receive and transmit flow control (default) – No flow control <p>Command mode: Interface port</p>
<pre>no shutdown</pre> <p>Enables the port.</p> <p>Command mode: Interface port</p>

Table 105. Management Port Configuration Commands (continued)

Command Syntax and Usage
<code>shutdown</code> Disables the port. Command mode: Interface port
<code>show interface port <port alias or number></code> Displays current port parameters. Command mode: All

Quality of Service Configuration

Quality of Service (QoS) commands configure the 802.1p priority value and DiffServ Code Point value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

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 106. CoPP Commands

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

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 150](#).

Table 107. WRED Configuration Options

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

Table 107. WRED Configuration Options

Command Syntax and Usage
<pre>no qos random-detect enable</pre> <p>Turns off Random Detection and avoidance.</p> <p>Command mode: Global configuration</p>
<pre>show qos random-detect</pre> <p>Displays current Random Detection and avoidance parameters.</p> <p>Command mode: All</p>

WRED Transmit Queue Configuration

Table 108. WRED Transmit Queue Options

Command Syntax and Usage
<pre>[no] qos random-detect transmit-queue <0-7> tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Global configuration</p>
<pre>[no] qos random-detect transmit-queue <0-7> non-tcp <min. threshold (1-100)> <max. threshold (1-100)> <drop rate (1-100)></pre> <p>Configures the WRED thresholds for non-TCP traffic. Use the <code>no</code> form to clear the WRED threshold value.</p> <p>Command mode: Global configuration</p>
<pre>qos random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>on</code>.</p> <p>Command mode: Global configuration</p>
<pre>no qos random-detect transmit-queue <0-7> enable</pre> <p>Sets the WRED transmit queue configuration to <code>off</code>.</p> <p>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 149](#).

Table 109. General ACL Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <1-640></pre> <p>Configures an Access Control List.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 156.</p>
<pre>[no] access-control group <1-640></pre> <p>Configures an ACL Group.</p> <p>Command mode: Global configuration</p> <p>To view command options, see page 164.</p>
<pre>show access-control</pre> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p>

Access Control List Configuration

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

Table 110. ACL Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <I-640> egress-port port <port alias or number></pre> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p>
<pre>access-control list <I-640> action {permit deny set-priority <0-7>}</pre> <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>
<pre>[no] access-control list <I-640> statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p>
<pre>default access-control list <I-640></pre> <p>Resets the ACL parameters to their default values.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list <I-640></pre> <p>Displays the current ACL parameters.</p> <p>Command mode: All</p>
<pre>[no] access-control list6 <I-128></pre> <p>Configures an IPv6 Access Control List. To view command options, see page 160.</p> <p>Command mode: Global configuration</p>

Ethernet Filtering Configuration

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

Table 111. Ethernet Filtering Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <1-640> ethernet source-mac-address <MAC address> <MAC mask></pre> <p>Defines the source MAC address for this ACL. Command mode: Global configuration</p>
<pre>[no] access-control list <1-640> ethernet destination-mac-address <MAC address> <MAC mask></pre> <p>Defines the destination MAC address for this ACL. Command mode: Global configuration</p>
<pre>[no] access-control list <1-640> ethernet vlan <VLAN ID> <VLAN mask></pre> <p>Defines a VLAN number and mask for this ACL. Command mode: Global configuration</p>
<pre>[no] access-control list <1-640> ethernet ethernet-type {arp ip ipv6 mpls rarp any <other (0x600-0xFFFF)>}</pre> <p>Defines the Ethernet type for this ACL. Command mode: Global configuration</p>
<pre>[no] access-control list <1-640> ethernet priority <0-7></pre> <p>Defines the Ethernet priority value for the ACL. Command mode: Global configuration</p>
<pre>default access-control list <1-640> ethernet</pre> <p>Resets Ethernet parameters for the ACL to their default values. Command mode: Global configuration</p>
<pre>no access-control list <1-640> ethernet</pre> <p>Removes Ethernet parameters for the ACL. Command mode: Global configuration</p>
<pre>show access-control list <1-640> ethernet</pre> <p>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 112. IP version 4 Filtering Configuration Commands

Command Syntax and Usage															
<pre>[no] access-control list <I-640> ipv4 source-ip-address <IP address> <IP mask></pre>	<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>														
<pre>[no] access-control list <I-640> ipv4 destination-ip-address <IP address> <IP mask></pre>	<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>														
<pre>[no] access-control list <I-640> ipv4 protocol <0-255></pre>	<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														
<pre>[no] access-control list <I-640> ipv4 type-of-service <0-255></pre>	<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>														
<pre>default access-control list <I-640> ipv4</pre>	<p>Resets the IPv4 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>														
<pre>show access-control list <I-640> ipv4</pre>	<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 113. TCP/UDP Filtering Configuration Commands

Command Syntax and Usage																													
<pre>[no] access-control list <1-640> tcp-udp source-port <1-65535> <mask (0xFFFF)></pre>	<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																												
<pre>[no] access-control list <1-640> tcp-udp destination-port <1-65535> <mask (0xFFFF)></pre>	<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>sport</code> above.</p> <p>Command mode: Global configuration</p>																												
<pre>[no] access-control list <1-640> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)></pre>	<p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p>																												
<pre>default access-control list <1-640> tcp-udp</pre>	<p>Resets the TCP/UDP parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>																												
<pre>show access-control list <1-640> tcp-udp</pre>	<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 114. Packet Format Filtering Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <I-640> packet-format ethernet {ethertype2 snap llc}</pre> <p>Defines the Ethernet format for the ACL.</p> <p>Command mode: Global configuration</p>
<pre>[no] access-control list <I-640> packet-format tagging {any none tagged}</pre> <p>Defines the tagging format for the ACL.</p> <p>Command mode: Global configuration</p>
<pre>[no] access-control list <I-640> packet-format ip {ipv4 ipv6}</pre> <p>Defines the IP format for the ACL.</p> <p>Command mode: Global configuration</p>
<pre>default access-control list <I-640> packet-format</pre> <p>Resets Packet Format parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list <I-640> packet-format</pre> <p>Displays the current Packet Format parameters for the ACL.</p> <p>Command mode: All</p>

ACL IPv6 Configuration

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

Table 115. IPv6 ACL Options

Command Syntax and Usage
<pre>[no] access-control list6 <I-128> egress-port port <port alias or number></pre> <p>Configures the ACL to function on egress packets.</p> <p>Command mode: Global configuration</p>
<pre>access-control list6 <I-128> action {permit deny set-priority <0-7>}</pre> <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>
<pre>[no] access-control list6 <I-128> statistics</pre> <p>Enables or disables the statistics collection for the Access Control List.</p> <p>Command mode: Global configuration</p>

Table 115. IPv6 ACL Options

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

IPv6 Filtering Configuration

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

Table 116. IP version 6 Filtering Options

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

Table 116. IP version 6 Filtering Options

Command Syntax and Usage
<pre>default access-control list6 <I-128> ipv6</pre> <p>Resets the IPv6 parameters for the ACL to their default values.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list6 <I-128> ipv6</pre> <p>Displays the current IPv6 parameters.</p> <p>Command mode: All</p>

IPv6 TCP/UDP Filtering Configuration

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

Table 117. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage																												
<pre>[no] access-control list6 <I-128> tcp-udp source-port <I-65535> <mask (0xFFFF)></pre> <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																											
<pre>[no] access-control list6 <I-128> tcp-udp destination-port <I-65535> <mask (0xFFFF)></pre> <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>sport</code> above.</p> <p>Command mode: Global configuration</p>																												
<pre>[no] access-control list6 <I-128> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)></pre> <p>Defines a TCP/UDP flag for the ACL.</p> <p>Command mode: Global configuration</p>																												

Table 117. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
<pre>default access-control list6 <I-128> tcp-udp</pre> <p>Resets the TCP/UDP parameters for the ACL to their default values. Command mode: Global configuration</p>
<pre>show access-control list6 <I-128> tcp-udp</pre> <p>Displays the current TCP/UDP Filtering parameters. Command mode: All</p>

IPv6 Re-Mark Configuration

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

IPv6 Re-Marking In-Profile Configuration

Table 118. IPv6 Re-Marking In-Profile Options

Command Syntax and Usage
<pre>[no] access-control list6 <I-128> re-mark dot1p <0-7></pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure. Command mode: Global configuration</p>
<pre>[no] access-control list6 <I-128> re-mark in-profile dscp <0-63></pre> <p>Re-marks the DSCP value for in-profile traffic. Command mode: Global configuration</p>
<pre>[no] access-control list6 <I-128> re-mark use-tos-precedence</pre> <p>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</p>
<pre>default access-control list6 <I-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values. Command mode: Global configuration</p>
<pre>show access-control list6 <I-128> re-mark</pre> <p>Displays current re-mark 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 119. ACL Group Configuration Commands

Command Syntax and Usage
<pre>access-control group <I-640> list <I-640></pre> <p>Adds the selected ACL to the ACL group. Command mode: Global configuration</p>
<pre>no access-control group <I-640> list <I-640></pre> <p>Removes the selected ACL from the ACL group. Command mode: Global configuration</p>
<pre>show access-control group <I-640></pre> <p>Displays the current ACL group parameters. Command mode: All</p>

ACL Metering Configuration

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

Table 120. ACL Metering Configuration Commands

Command Syntax and Usage
<pre>access-control list <I-640> meter committed-rate <64-10000000></pre> <p>Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. Command mode: Global configuration</p>
<pre>access-control list <I-640> meter maximum-burst-size <32-4096></pre> <p>Configures the maximum burst size, in Kilobits. Enter one of the following values for mbsize: 32, 64, 128, 256, 512, 1024, 2048, 4096 Command mode: Global configuration</p>
<pre>[no] access-control list <I-640> meter enable</pre> <p>Enables or disables ACL Metering. Command mode: Global configuration</p>
<pre>access-control list <I-640> meter action {drop pass}</pre> <p>Configures the ACL meter to either drop or pass out-of-profile traffic. Command mode: Global configuration</p>
<pre>default access-control list <I-640> meter</pre> <p>Sets the ACL meter configuration to its default values. Command mode: Global configuration</p>

Table 120. ACL Metering Configuration Commands

Command Syntax and Usage
<pre>[no] access-control list <1-640> meter log</pre> <p>Configures the ACL meter to log out-of-profile notifications. Command mode: Global configuration</p>
<pre>no access-control list <1-640> meter</pre> <p>Deletes the selected ACL meter. Command mode: Global configuration</p>
<pre>show access-control list <1-640> meter</pre> <p>Displays current ACL Metering parameters. Command mode: All</p>

ACL Re-Mark Configuration

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

Table 121. ACL Re-Marking Configuration Commands

Command Syntax and Usage
<pre>access-control list <1-640> re-mark dot1p <0-7></pre> <p>Defines 802.1p value. The value is the priority bits information in the packet structure. Command mode: Global configuration</p>
<pre>no access-control list <1-640> re-mark dot1p</pre> <p>Disables use of 802.1p value for re-marked packets. Command mode: Global configuration</p>
<pre>[no] access-control list <1-640> re-mark use-tos-precedence</pre> <p>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</p>
<pre>default access-control list <1-640> re-mark</pre> <p>Sets the ACL Re-mark configuration to its default values. Command mode: Global configuration</p>
<pre>show access-control list <1-640> re-mark</pre> <p>Displays current Re-mark parameters. Command mode: All</p>

Re-Marking In-Profile Configuration

Table 122. ACL Re-Mark In-Profile Commands

Command Syntax and Usage
<pre>access-control list <1-640> re-mark in-profile dscp <0-63></pre> <p>Sets the DiffServ Code Point (DSCP) of in-profile packets to the selected value.</p> <p>Command mode: Global configuration</p>
<pre>no access-control list <1-640> re-mark in-profile dscp</pre> <p>Disables use of DSCP value for in-profile traffic.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list <1-640> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p>

Re-Marking Out-of-Profile Configuration

Table 123. ACL Re-Mark Out-of-Profile Commands

Command Syntax and Usage
<pre>access-control list <1-640> re-mark out-profile dscp <0-63></pre> <p>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.</p> <p>Command mode: Global configuration</p>
<pre>no access-control list <1-640> re-mark out-profile dscp</pre> <p>Disables use of DSCP value for out-of-profile traffic.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list <1-640> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p>

IPv6 Re-Marking Configuration

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

Table 124. IPv6 General Re-Mark Options

Command Syntax and Usage
<pre>[no] access-control list6 <1-128> re-mark dot1p <0-7></pre> <p>Re-marks the 802.1p value. The value is the priority bits information in the packet structure.</p> <p>Command mode: Global configuration</p>
<pre>[no] no access-control list6 <1-128> re-mark use-tos-precedence</pre> <p>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.</p> <p>Command mode: Global configuration</p>
<pre>default access-control list6 <1-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values.</p> <p>Command mode: Global configuration</p>
<pre>show access-control list6 <1-128> re-mark</pre> <p>Displays current re-mark parameters.</p> <p>Command mode: All</p>

IPv6 Re-Marking In-Profile Configuration

Table 125. IPv6 Re-Mark In-Profile Options

Command Syntax and Usage
<pre>[no] access-control list6 <1-128> re-mark in-profile dscp <0-63></pre> <p>Re-marks the DSCP value for in-profile traffic. Command mode: Global configuration</p>
<pre>default access-control list6 <1-128> re-mark</pre> <p>Sets the ACL re-mark parameters to their default values. Command mode: Global configuration</p>
<pre>show access-control list6 <1-128> re-mark</pre> <p>Displays current re-mark parameters. 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 126. Layer 2 Configuration Commands

Command Syntax and Usage
<pre>show layer2</pre> <p>Displays current Layer 2 parameters.</p> <p>Command mode: All</p>

Forwarding Database Configuration

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

Table 127. FDB Configuration Commands

Command Syntax and Usage
<pre>mac-address-table aging <0-65535></pre> <p>Configures the aging value for FDB entries, in seconds. The default value is 300.</p> <p>Command mode: Global configuration</p>
<pre>[no] mac-address-table mac-notification</pre> <p>Enables or disables MAC address notification.</p> <p>Command mode: Global configuration</p>
<pre>show mac-address-table</pre> <p>Display current FDB configuration.</p> <p>Command mode: All</p>

Static FDB Configuration

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

Table 128. FDB Configuration Commands

Command Syntax and Usage
<pre>mac-address-table static <MAC address> vlan <VLAN number> {port <port alias or number> portchannel <trunk number> adminkey <1-65535>}</pre> <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: xxxxxxxxxxxxxx</p> <p>For example, 080020123456</p> <p>Command mode: Global configuration</p>
<pre>no mac-address-table static <MAC address> <VLAN number></pre> <p>Deletes a permanent FDB entry.</p> <p>Command mode: Global configuration</p>
<pre>show mac-address-table</pre> <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 129. LLDP Configuration Commands

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

Table 129. LLDP Configuration Commands

Command Syntax and Usage
<pre>lldp transmission-delay <1-8192></pre> <p>Configures the transmission delay interval. The transmit delay timer represents the minimum time permitted between successive LLDP transmissions on a port.</p> <p>The default value is 2.</p> <p>Command mode: Global configuration</p>
<pre>lldp reinit-delay <1-10></pre> <p>Configures the re-initialization delay interval, in seconds. The re-initialization delay allows the port LLDP information to stabilize before transmitting LLDP messages.</p> <p>The default value is 2.</p> <p>Command mode: Global configuration</p>
<pre>lldp enable</pre> <p>Globally turns LLDP on. The default setting is on.</p> <p>Command mode: Global configuration</p>
<pre>no lldp enable</pre> <p>Globally turns LLDP off.</p> <p>Command mode: Global configuration</p>
<pre>show lldp</pre> <p>Display current LLDP configuration.</p> <p>Command mode: All</p>

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 130. LLDP Port Commands

Command Syntax and Usage
<pre>lldp admin-status {disabled tx_only rx_only tx_rx}</pre> <p>Configures the LLDP transmission type for the port, as follows:</p> <ul style="list-style-type: none"> – Transmit only – Receive only – Transmit and receive – Disabled <p>The default setting is tx_rx.</p> <p>Command mode: Interface port</p>

Table 130. LLDP Port Commands

Command Syntax and Usage
<pre>[no] lldp trap-notification</pre> <p>Enables or disables SNMP trap notification for LLDP messages.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number> lldp</pre> <p>Display current LLDP port configuration.</p> <p>Command mode: All</p>

LLDP Optional TLV configuration

Use the following commands to configure LLDP port TLV (Type, Length, Value) options for the selected port.

Table 131. Optional TLV Commands

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

Table 131. Optional TLV Commands (continued)

Command Syntax and Usage
<pre>[no] lldp tlv powermdi</pre> <p>Enables or disables the Power via MDI information type. Command mode: Interface port</p>
<pre>[no] lldp tlv linkaggr</pre> <p>Enables or disables the Link Aggregation information type. Command mode: Interface port</p>
<pre>[no] lldp tlv framesz</pre> <p>Enables or disables the Maximum Frame Size information type. Command mode: Interface port</p>
<pre>[no] lldp tlv dcbx</pre> <p>Enables or disables the Data Center Bridging Capability Exchange (DCBX) information type. Command mode: Interface port</p>
<pre>[no] lldp tlv all</pre> <p>Enables or disables all optional TLV information types. Command mode: Interface port</p>
<pre>show interface port <port alias or number> lldp</pre> <p>Display current LLDP port configuration. Command mode: All</p>

Trunk Configuration

Trunk groups can provide super-bandwidth connections between S14093 or other trunk capable devices. A *trunk* is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 64 trunk groups can be configured on the S14093, with the following restrictions:

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

By default, each trunk group is empty and disabled.

Table 132. Trunk Configuration Commands

Command Syntax and Usage	
<pre>portchannel <1-64> port <port alias or number></pre>	<p>Adds a physical port or ports to the current trunk group. You can add several ports, with each port separated by a comma (,) or a range of ports, separated by a dash (-).</p> <p>Command mode: Global configuration</p>
<pre>no portchannel <1-64> port <port alias or number></pre>	<p>Removes a physical port or ports from the current trunk group.</p> <p>Command mode: Global configuration</p>
<pre>[no] portchannel <1-64> enable</pre>	<p>Enables or Disables the current trunk group.</p> <p>Command mode: Global configuration</p>
<pre>no portchannel <1-64></pre>	<p>Removes the current trunk group configuration.</p> <p>Command mode: Global configuration</p>
<pre>show portchannel <1-64></pre>	<p>Displays current trunk group parameters.</p> <p>Command mode: All</p>

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the SI4093. Trunk hash parameters are set globally for the SI4093. The trunk hash settings affect both static trunks and LACP trunks.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in [Table 133](#) combined with the hash parameters listed in [Table 134](#).

Table 133. Trunk Hash Settings

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

Layer 2 Trunk Hash

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

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

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

Table 134. Layer 2 Trunk Hash Options

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

Table 134. Layer 2 Trunk Hash Options (continued)

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

Layer 3 Trunk Hash

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

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

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

Table 135. Layer 3 Trunk Hash Options

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

Link Aggregation Control Protocol Configuration

Use the following commands to configure Link Aggregation Control Protocol (LACP) for the SI4093.

Table 136. Link Aggregation Control Protocol Commands

Command Syntax and Usage	
<pre>lacp system-priority <I-65535></pre>	<p>Defines the priority value for the SI4093. Lower numbers provide higher priority. The default value is 32768.</p> <p>Command mode: Global configuration</p>
<pre>lacp timeout {short long}</pre>	<p>Defines the timeout period before invalidating LACP data from a remote partner. Choose <i>short</i> (3 seconds) or <i>long</i> (90 seconds). The default value is <i>long</i>.</p> <p>Note: It is recommended that you use a timeout value of <i>long</i>, to reduce LACPDU processing. If your SI4093's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.</p> <p>Command mode: Global configuration</p>
<pre>default lacp [system-priority timeout]</pre>	<p>Restores either the VFSM priority value, timeout period or both to their default values.</p> <p>Command mode: Global configuration</p>
<pre>no lacp <I-65535></pre>	<p>Deletes a selected LACP trunk, 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>
<pre>portchannel <trunk ID> lacp key <I-65535> suspend-individual</pre>	<p>Enables a static LACP trunk. In this mode, ports sharing the same LACP admin key can form a single trunk, with the specified <i>trunk ID</i>. The active trunk is picked based on the ports which occupy first the trunk ID. Member ports that cannot join this trunk are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic.</p> <p>Command mode: Global configuration</p>
<pre>no portchannel <trunk ID></pre>	<p>Disables a static LACP trunk.</p> <p>Command mode: Global configuration</p>
<pre>show lacp</pre>	<p>Display current LACP configuration.</p> <p>Command mode: All</p>

LACP Port Configuration

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

Table 137. Link Aggregation Control Protocol Commands

Command Syntax and Usage
<pre>lacp mode {off active passive}</pre> <p>Set the LACP mode for this port, as follows:</p> <ul style="list-style-type: none"> – off Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is <i>off</i>. – active Turn LACP on and set this port to active. Active ports initiate LACPDU's. – passive Turn LACP on and set this port to passive. Passive ports do not initiate LACPDU's, but respond to LACPDU's from active ports. <p>Command mode: Interface port</p>
<pre>lacp priority <1-65535></pre> <p>Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.</p> <p>Command mode: Interface port</p>
<pre>lacp key <1-65535></pre> <p>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 trunk group.</p> <p>Command mode: Interface port</p>
<pre>port-channel min-links <1-></pre> <p>Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the <i>down</i> state.</p> <p>Command mode: Interface port</p>
<pre>default lacp [key mode priority]</pre> <p>Restores the selected parameters to their default values.</p> <p>Command mode: Interface port</p>
<pre>show interface port <port alias or number> lacp</pre> <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 *IBM Networking OS Application Guide*.

Table 138. Layer 2 Failover Configuration Commands

Command Syntax and Usage
<pre>failover enable</pre> <p>Globally turns Layer 2 Failover on.</p> <p>Command mode: Global configuration</p>
<pre>no failover enable</pre> <p>Globally turns Layer 2 Failover off.</p> <p>Command mode: Global configuration</p>
<pre>show failover trigger</pre> <p>Displays current Layer 2 Failover parameters.</p> <p>Command mode: All</p>

Failover Trigger Configuration

Table 139. Failover Trigger Configuration Commands

Command Syntax and Usage
<pre>[no] failover trigger <1-8> enable</pre> <p>Enables or disables the Failover trigger.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <1-8></pre> <p>Deletes the Failover trigger.</p> <p>Command mode: Global configuration</p>
<pre>failover trigger <1-8> limit <0-1024></pre> <p>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.</p> <p>Command mode: Global configuration</p>
<pre>show failover trigger <1-8></pre> <p>Displays the current failover trigger settings.</p> <p>Command mode: All</p>

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 140. Failover Manual Monitor Port Commands

Command Syntax and Usage
<pre>failover trigger <1-8> mmon monitor member <port alias or number></pre> <p>Adds the selected port to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <1-8> mmon monitor member <port alias or number></pre> <p>Removes the selected port from the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>failover trigger <1-8> mmon monitor portchannel <trunk number></pre> <p>Adds the selected trunk group to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <1-8> mmon monitor portchannel <trunk number></pre> <p>Removes the selected trunk group to the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>failover trigger <1-8> mmon monitor adminkey <1-65535></pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Port configuration. LACP trunks formed with this <i>admin key</i> will be included in the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <1-8> mmon monitor adminkey <1-65535></pre> <p>Removes an LACP admin key from the Manual Monitor Port configuration.</p> <p>Command mode: Global configuration</p>
<pre>show failover trigger <1-8></pre> <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 141. Failover Manual Monitor Control Commands

Command Syntax and Usage
<pre>failover trigger <I-8> mmon control member <port alias or number></pre> <p>Adds the selected port to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <I-8> mmon control member <port alias or number></pre> <p>Removes the selected port from the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>failover trigger <I-8> mmon control portchannel <trunk number></pre> <p>Adds the selected trunk group to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <I-8> mmon control portchannel <trunk number></pre> <p>Removes the selected trunk group to the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>failover trigger <I-8> mmon control adminkey <I-65535></pre> <p>Adds an LACP <i>admin key</i> to the Manual Monitor Control configuration. LACP trunks formed with this <i>admin key</i> will be included in the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>no failover trigger <I-8> mmon control adminkey <I-65535></pre> <p>Removes an LACP admin key from the Manual Monitor Control configuration.</p> <p>Command mode: Global configuration</p>
<pre>show failover trigger <I-8></pre> <p>Displays the current Failover settings.</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 142. Layer 3 Configuration Commands

Command Syntax and Usage
<pre>interface ip <interface number></pre> <p>Configures the IP Interface. The SI4093 supports up to 4 IP interfaces. To view command options, see page 184.</p> <p>Command mode: Global configuration</p>
<pre>show layer3</pre> <p>Displays the current IP configuration.</p> <p>Command mode: All</p>

IP Interface Configuration

The SI4093 supports up to 4 IP interfaces. Each IP interface represents the SI4093 on an IP subnet on your network. The Interface option is disabled by default.

IP Interface 127 and 4 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 143. IP Interface Configuration Commands

Command Syntax and Usage	
<code>interface ip <interface number></code>	Enter IP interface mode. Command mode: Global configuration
<code>ip address <IP address> [<IP netmask>]</code>	Configures the IP address of the switch interface, using dotted decimal notation. Command mode: Interface IP
<code>ip netmask <IP netmask></code>	Configures the IP subnet address mask for the interface, using dotted decimal notation. Command mode: Interface IP
<code>vlan <VLAN number></code>	Configures the VLAN number for this interface. Each interface can belong to one VLAN. Command mode: Interface IP
<code>[no] relay</code>	Enables or disables the BOOTP relay on this interface. The default setting is enabled. Command mode: Interface IP
<code>enable</code>	Enables this IP interface. Command mode: Interface IP
<code>no enable</code>	Disables this IP interface. Command mode: Interface IP

Table 143. IP Interface Configuration Commands (continued)

Command Syntax and Usage
<pre>no interface ip <interface number></pre> <p>Removes this IP interface.</p> <p>Command mode: Interface IP</p>
<pre>show interface ip <interface number></pre> <p>Displays the current interface settings.</p> <p>Command mode: All</p>

Default Gateway Configuration

The switch can be configured with up to 4 IPv4 gateways. Gateways 3–4 are reserved for default gateways. Gateway 4 is reserved for switch management. Default gateway indices are:

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

This option is disabled by default.

Table 144. Default Gateway Configuration Commands

Command Syntax and Usage	
<code>ip gateway <3-4> address <IP address></code>	Configures the IP address of the default IP gateway using dotted decimal notation. Default gateway indices are: Command mode: Global configuration
<code>ip gateway <3-4> interval <0-60></code>	The switch pings the default gateway to verify that it's up. This command sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds. Command mode: Global configuration
<code>ip gateway <3-4> retry <1-120></code>	Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts. Command mode: Global configuration
<code>[no] ip gateway <3-4> arp-health-check</code>	Enables or disables Address Resolution Protocol (ARP) health checks. The default setting is disabled. The <code>arp</code> option does not apply to management gateways. Command mode: Global configuration
<code>ip gateway <3-4> enable</code>	Enables the gateway for use. Command mode: Global configuration
<code>no ip gateway <3-4> enable</code>	Disables the gateway. Command mode: Global configuration
<code>no ip gateway <3-4></code>	Deletes the gateway from the configuration. Command mode: Global configuration
<code>show ip gateway <3-4></code>	Displays the current gateway settings. Command mode: All

Network Filter Configuration

Table 145. IP Network Filter Configuration Commands

Command Syntax and Usage
<pre>ip match-address <1-256> enable</pre> <p>Enables the Network Filter configuration. Command mode: Global configuration</p>
<pre>no ip match-address <1-256> enable</pre> <p>Disables the Network Filter configuration. Command mode: Global configuration</p>
<pre>no ip match-address <1-256></pre> <p>Deletes the Network Filter configuration. Command mode: Global configuration</p>
<pre>show ip match-address [<1-256>]</pre> <p>Displays the current the Network Filter configuration. Command mode: All</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 146. Domain Name Service Commands

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

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 132 is reserved for management.

[Table 147](#) describes the IPv6 Default Gateway Configuration commands.

Table 147. IPv6 Default Gateway Configuration Commands

Command Syntax and Usage
<pre>ip gateway6 {<gateway number>} address <IPv6 address></pre> <p>Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:abcd:12).</p> <p>Command mode: Global configuration</p>
<pre>[no] ip gateway6 {<gateway number>} enable</pre> <p>Enables or disables the default gateway.</p> <p>Command mode: Global configuration</p>
<pre>no ip gateway6 {<gateway number>}</pre> <p>Deletes the default gateway.</p> <p>Command mode: Global configuration</p>
<pre>show ipv6 gateway6 {<gateway number>}</pre> <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 148. IPv6 Path MTU Commands

Command Syntax and Usage
<pre>ip pmtu6 timeout 0 <10-100></pre> <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 minutes.</p> <p>Command mode: Global configuration</p>
<pre>clear ipv6 pmtu</pre> <p>Clears all entries in the Path MTU cache.</p> <p>Command mode: All Except User EXEC</p>
<pre>show ipv6 pmtu</pre> <p>Displays the current Path MTU configuration.</p> <p>Command mode: All</p>

IPv6 Neighbor Discovery Prefix Configuration

The following table describes the Neighbor Discovery prefix configuration options. These commands allow you to define a list of prefixes to be placed in Prefix Information options in Router Advertisement messages sent from an interface.

Table 149. IPv6 Neighbor Discovery Prefix Commands

Command Syntax and Usage
<pre>interface ip <I25-I27></pre> <p>Enters Interface IP mode.</p> <p>Command mode: Global configuration</p>
<pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} [no-advertise]</pre> <p>Adds a Neighbor Discovery prefix to the interface. The default setting is enabled.</p> <p>To disable the prefix and not advertise it in the Prefix Information options in Router Advertisement messages sent from the interface use the <code>no-advertise</code> option.</p> <p>Additional prefix options are listed in this table.</p> <p>Command mode: Interface IP</p>
<pre>no ipv6 nd prefix [<IPv6 prefix> <prefix length>] interface all</pre> <p>Removes the selected Neighbor Discovery prefix(es). If you specify an interface number, all prefixes for the interface are removed.</p> <p>Command mode: Interface IP</p>
<pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} valid-lifetime <0-4294967295> [infinite variable] preferred-lifetime <0-4294967295> [infinite variable]</pre> <p>Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.</p> <p>The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The default value is 2592000.</p> <p>The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The default value is 604800.</p> <p>Note: The Preferred Lifetime value must not exceed the Valid Lifetime value.</p> <p>Command mode: Interface IP</p>
<pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} off-link [no-autoconfig]</pre> <p>Disables the on-link flag. When enabled, the on-link flag indicates that this prefix can be used for on-link determination. When disabled, the advertisement makes no statement about on-link or off-link properties of the prefix. The default setting is enabled.</p> <p>To clear the off-link flag, omit the off-link parameter when you issue this command.</p> <p>Command mode: Interface IP</p>

Table 149. IPv6 Neighbor Discovery Prefix Commands (continued)

Command Syntax and Usage
<pre>ipv6 nd prefix {<IPv6 prefix> <prefix length>} no-autoconfig</pre> <p>Disables the autonomous flag. When enabled, the autonomous flag indicates that the prefix can be used for stateless address configuration. The default setting is enabled.</p> <p>Command mode: Interface IP</p>
<pre>show ipv6 prefix {<interface number>}</pre> <p>Displays current Neighbor Discovery prefix parameters.</p> <p>Command mode: All</p>

IPv6 Prefix Policy Table Configuration

The following table describes the configuration options for the IPv6 Prefix Policy Table. The Prefix Policy Table allows you to override the default address selection criteria.

Table 150. IPv6 Prefix Policy Table Options

Command Syntax and Usage
<pre>ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)></pre> <p>Adds a Prefix Policy Table entry. Enter the following parameters:</p> <ul style="list-style-type: none"> – IPv6 address prefix – Prefix length – Precedence: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence. – Label: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match. <p>Command mode: Global configuration</p>
<pre>no ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)></pre> <p>Removes a prefix policy table entry.</p> <p>Command mode: Global configuration</p>
<pre>show ip prefix-policy</pre> <p>Displays the current Prefix Policy Table configuration.</p> <p>Command mode: All</p>

Converged Enhanced Ethernet Configuration

Table 151 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 151. CEE Commands

Command Syntax and Usage
<code>cee enable</code> Globally turns CEE on. Command mode: Global configuration
<code>no cee enable</code> Globally turns CEE off. Command mode: Global configuration
<code>cee iscsi enable</code> Enables or disables ISCSI TLV advertisements. Command mode: Global configuration
<code>show cee iscsi</code> Displays the current ISCSI TLV parameters. Command mode: All
<code>show cee</code> Displays the current CEE parameters. Command mode: All

ETS Global Configuration

Enhanced Transmission Selection (ETS) allows you to allocate bandwidth to different traffic types, based on 802.1p priority.

Note: ETS configuration supersedes the QoS 802.1p menu. When ETS is enabled, you cannot configure the 802.1p menu options.

ETS Global Priority Group Configuration

Table 152 describes the global ETS Priority Group configuration options.

Table 152. Global ETS Priority Group Commands

Command Syntax and Usage
<pre>cee global ets priority-group pgid <0-7, 15> bandwidth <802.1p priority (0-7)> <bandwidth percentage (0, 10-100)></pre> <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>
<pre>cee global ets priority-group pgid <0-7, 15> description <1-31 characters></pre> <p>Enter text that describes this Priority Group.</p> <p>Command mode: Global configuration</p>
<pre>no cee global ets priority-group <0-7, 15> description</pre> <p>Removes the description for the specified Priority Group.</p> <p>Command mode: Global configuration</p>
<pre>[no] cee global ets mcast-priority-group mcpgid <0-3> [bandwidth percentage <0, 10-100>] [priority <0-7>]</pre> <p>Configures Multicast Priority Group parameters. You can enter the link bandwidth percentage allocated to the Multicast Priority Group, and assign one or more 802.1p values to the Multicast Priority Group.</p> <p>Command mode: Global configuration</p>
<pre>cee global ets mcast-priority-group mcpgid <0-3> description <1-31 characters></pre> <p>Enter text that describes the multicast priority group.</p> <p>Command mode: Global configuration</p>
<pre>no cee global ets mcast-priority-group mcpgid <0-3> description</pre> <p>Removes the description for the specified multicast priority group.</p> <p>Command mode: Global configuration</p>
<pre>cee global ets priority-group pgid <0-7, 15> priority <0-7></pre> <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>

Table 152. Global ETS Priority Group Commands

Command Syntax and Usage
<pre>show cee global ets priority-group <0-7, 15></pre> <p>Displays the current global ETS Priority Group parameters. Command mode: All</p>
<pre>show cee global ets</pre> <p>Displays the current global ETS Priority Group parameters. Command mode: All</p>
<pre>show cee global ets mcast-priority-group <0-3></pre> <p>Displays the current global ETS Multicast Priority Group parameters. 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.

Port-level 802.1p PFC Configuration

Table 153 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 153. Port 802.1p PFC Options

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

Table 153. Port 802.1p PFC Options (continued)

Command Syntax and Usage
<pre>show cee port <port alias or number> pfc priority <0-7></pre> <p>Displays the current 802.1p PFC parameters for the selected port.</p> <p>Command mode: All</p>
<pre>show cee port <port alias or number> pfc</pre> <p>Displays the current PFC parameters for the selected port.</p> <p>Command mode: All</p>

DCBX Port Configuration

Table 154 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 154. Port DCBX Commands

Command Syntax and Usage
<pre>[no] cee port <port alias or number> dcbx app_proto advertise</pre> <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>
<pre>[no] cee port <port alias or number> dcbx app_proto willing</pre> <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>
<pre>[no] cee port <port alias or number> dcbx ets advertise</pre> <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>
<pre>[no] cee port <port alias or number> dcbx ets willing</pre> <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>
<pre>[no] cee port <port alias or number> dcbx pfc advertise</pre> <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>
<pre>[no] cee port <port alias or number> dcbx pfc willing</pre> <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>

Table 154. Port DCBX Commands (continued)

Command Syntax and Usage
<pre>no cee port <port alias or number> dcbx enable</pre> <p>Disables DCBX on the port. Command mode: Global configuration</p>
<pre>cee port <port alias or number> dcbx enable</pre> <p>Enables DCBX on the port. Command mode: Global configuration</p>
<pre>show cee port <port alias or number> dcbx</pre> <p>Displays the current port DCBX parameters. 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 155 describes the FCoE configuration options.

Table 155. FCoE Configuration Commands

Command Syntax and Usage
<code>fcoe fips enable</code> Globally turns FIP Snooping on. Command mode: Global configuration
<code>no fcoe fips enable</code> Globally turns FIP Snooping off. Command mode: Global configuration
<code>[no] fcoe fips timeout-acl</code> 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
<code>show fcoe information</code> 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 156](#) describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 156. Port FIP Snooping Commands

Command Syntax and Usage
<pre>fcoe fips port <port alias or number> fcf-mode [auto on off]</pre> <p>Configures FCoE Forwarding (FCF) on the port, as follows:</p> <ul style="list-style-type: none">– on: Configures the port as a Fibre Channel Forwarding (FCF) port.– off: Configures the port as an FCoE node (ENode).– auto: Automatically detect the configuration of the connected device, and configure this port to match. <p>Command mode: Global configuration</p>
<pre>fcoe fips port <port alias or number> enable</pre> <p>Enables FIP Snooping on the port. 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>
<pre>no fcoe fips port <port alias or number> enable</pre> <p>Disables FIP Snooping on the port.</p> <p>Command mode: Global configuration</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 157. 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
[no] uplink {port <port no.> portchannel <1-64> adminkey <1-65535>}	Enables or disables uplink connectivity for the SPAR. A single external port, portchannel, or LACP channel can be used for uplink. All uplinks within a SPAR are automatically assigned to the SPAR domain's default VLAN and to any SPAR local VLANs. Command mode: SPAR Configuration
domain default {vlan <2-4094> member <port no.>}	Configures the SPAR's default domain settings: <ul style="list-style-type: none"> – 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. – 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 157. SPAR Configuration Options (continued)

Command Syntax and Usage
<pre>domain local <1-32> {enable member <port no.> name <text> vlan <2-4094>}</pre> <p>Configures the SPAR's local domains:</p> <ul style="list-style-type: none"> – enable enables the SPAR local domains – member adds server ports to the SPAR local domains – name configures the SPAR local domains names – vlan applies a VLAN ID to the SPAR local domains. The default value is 0. <p>Command mode: SPAR Configuration</p>
<pre>no domain local <1-32> [enable member <port no.>]</pre> <p>Deletes the SPAR local VLAN domains:</p> <ul style="list-style-type: none"> – enable disables the SPAR local domains – member deletes SPAR local domains server ports <p>Command mode: SPAR Configuration</p>
<pre>domain mode {passthrough local}</pre> <p>Configures the SPAR domain mode:</p> <ul style="list-style-type: none"> – 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. – 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>
<pre>show spar <1-8> [domain [default local <1-32>] uplink]</pre> <p>Displays the SPAR settings:</p> <ul style="list-style-type: none"> – domain filters only the SPAR domain related settings <ul style="list-style-type: none"> • default filters only SPAR default domain settings • local <1-32> filters only SPAR local domains settings – 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 10Gb System Interconnect Module behaves as a Service Agent providing systems management services.

Table 158. Service Location Protocol

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

Configuration Dump

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

```
Router(config)# show running-config
```

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on [page 204](#).

Saving the Active Switch Configuration

When the `copy running-config {ftp|tftp|sftp}` command is used, the switch's active configuration commands (as displayed using `show running-config`) will be uploaded to the specified script configuration file on the FTP/TFTP/SFTP server. To start the switch configuration upload, at the prompt, enter:

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

```
Router(config)# copy ftp running-config [extm-port|mgt-port]
    or
Router(config)# copy tftp running-config [extm-port|mgt-port]
    or
Router(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 159. General Operations Commands

Command Syntax and Usage
<pre>password <1-128 characters></pre> <p>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.</p> <p>Command Mode: Privileged EXEC</p>
<pre>clear logging</pre> <p>Clears all Syslog messages.</p> <p>Command Mode: Privileged EXEC</p>
<pre>ntp send</pre> <p>Allows the user to send requests to the NTP server.</p> <p>Command Mode: Privileged EXEC</p>

Operations-Level Port Commands

Operations-level port options are used for temporarily disabling or enabling a port, and for re-setting the port.

Table 160. Port Operations Commands

Command Syntax and Usage
<pre>no interface port <port number or alias> shutdown</pre> <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>
<pre>interface port <port number or alias> shutdown</pre> <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>
<pre>show interface port <port number or alias> operation</pre> <p>Displays the port interface operational state.</p> <p>Command Mode: Privileged EXEC</p>

Operations-Level FCoE Commands

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

Table 161. FCoE Operations Commands

Command Syntax and Usage
<pre>no fcoe fips fcf <MAC address></pre> <p>Deletes the selected FCoE Forwarder (FCF), and any associated ACLs.</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 162. Protected Mode Options

Command Syntax and Usage
<pre>[no] protected-mode external-management</pre> <p>Enables exclusive local control of switch management. When Protected Mode is set to <code>on</code>, the management module cannot be used to disable external management on the switch. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<pre>[no] protected-mode external-ports</pre> <p>Enables exclusive local control of external ports. When Protected Mode is set to <code>on</code>, the management module cannot be used to disable external ports on the switch. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<pre>[no] protected-mode factory-default</pre> <p>Enables exclusive local control of factory default resets. When Protected Mode is set to <code>on</code>, the management module cannot be used to reset the switch software to factory default values. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<pre>[no] protected-mode management-vlan-interface</pre> <p>Enables exclusive local control of the management interface. When Protected Mode is set to <code>on</code>, the management module cannot be used to configure parameters for the management interface. The default value is <code>enabled</code>.</p> <p>Note: Due to current management module implementation, this setting cannot be disabled.</p> <p>Command Mode: Global Configuration</p>
<pre>protected-mode enable</pre> <p>Turns Protected Mode <code>on</code>. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.</p> <p>Command Mode: Global Configuration</p>

Table 162. Protected Mode Options (continued)

Command Syntax and Usage
<pre>no protected-mode enable</pre> <p>Turns Protected Mode <i>off</i>. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.</p> <p>Command Mode: Global Configuration</p>
<pre>show protected-mode</pre> <p>Displays the current Protected Mode configuration.</p> <p>Command Mode: Global Configuration</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 163. Boot Scheduling Options

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

Netboot Configuration

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

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

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

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

Table 164. Netboot Options (/boot/netboot)

Command Syntax and Usage	
<code>boot netboot enable</code>	<p>Enables 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>
<code>no boot netboot enable</code>	<p>Disables Netboot.</p> <p>Command mode: Global configuration</p>
<code>[no] boot netboot tftp <IP address></code>	<p>Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled, or if the DHCP server does not return the required information.</p> <p>Command mode: Global configuration</p>
<code>[no] boot netboot cfgfile <1-31 characters></code>	<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>
<code>show boot</code>	<p>Displays the current Netboot parameters.</p> <p>Command mode: All</p>

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 165. Netboot Options (/boot/qsfp-40Gports)

Command Syntax and Usage
<pre>[no] boot qsfp-40Gports <ports></pre> <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>
<pre>show boot qsfp-port-modes</pre> <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 10Gb System Interconnect Module. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your SI4093, go to:

<http://www-304.ibm.com/jct01004c/systems/support>

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

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP or TFTP server on your network
- Transferring the new image from the FTP or TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

Loading New Software to Your Switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To load a new software image to your switch, you need the following:

- The image or boot software loaded on an FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames.

When the above requirements are met, use the following procedure to download the new software to your switch.

1. In Privileged EXEC mode, enter the following command:

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

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

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

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

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

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

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

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

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

5. The system prompts you to confirm your request.

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

Selecting a Software Image to Run

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

1. In Global Configuration mode, enter:

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

2. Enter the name of the image you want the switch to use upon the next boot. The system informs you of which image set to be loaded at the next reset:

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

Uploading a Software Image from Your Switch

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

1. In Privileged EXEC mode, enter:

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

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

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

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

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

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

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

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

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

```
image2 currently contains Software Version 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 10Gb System Interconnect Module, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform a save operation (`copy running-config startup-config`), your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your SI4093 10Gb System Interconnect Module was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured SI4093 10Gb System Interconnect Module is moved to a network environment where it will be re-configured for a different purpose.

In Global Configuration mode, use the following command to set which configuration block you want the switch to load the next time it is reset:

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

Resetting the Switch

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

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

```
>> Router# reload
```

You are prompted to confirm your request.

```
Reset will use software "image2" and the active config block.  
Confirm reload (y/n) ?
```

Changing the Switch Profile

The IBM Networking OS software for the SI4093 can be configured to operate in different modes for different deployment scenarios. The deployment profile changes some of the basic switch behavior, shifting switch resources to optimize capacity levels to meet the needs of different types of networks. For more information about deployment profiles, see the IBM Networking OS 7.7 *Application Guide*.

To change the deployment profile, select the new profile and reset the SI4093. Use the following command to select a new profile:

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

Using the Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

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

Boot Management Menu
1 - Change booting image
2 - Change configuration block
3 - Xmodem download
4 - Exit

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

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

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform an Xmodem download, press 3 and follow the screen prompts.
- To exit the Boot Management menu, press 4. The booting process continues.

Recovering from a Failed Software Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports XModem Download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 bps
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing **<Shift B>** while the Memory Test is in progress and the dots are being displayed.
4. Select **3** for **Xmodem download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

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

5. Press **<Enter>** to set the system into download accept mode. When the readiness meter displays (a series of "C" characters), start XModem on your terminal emulator.

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

```
yzModem - CRC mode, 62494 (SOH)/0 (STX)/0 (CAN) packets, 6 retries
Extracting images ... Do *NOT* power cycle the switch.
**** VMLINUX ****
Un-Protected 10 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 10 sectors
**** RAMDISK ****
Un-Protected 44 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 44 sectors
**** BOOT CODE ****
Un-Protected 8 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 8 sectors
```

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

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

8. Press the Escape key (<Esc>) to re-display the Boot Management menu.
9. Select **3** to start a new **XModem Download**. When you see the following message, change the Serial Port characteristics to 115200 bps:

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

10. Press <Enter> to continue the download.

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

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries
Extracting images ... Do *NOT* power cycle the switch.
**** Switch OS ****
Please choose the Switch OS Image to upgrade [1|2|n] :
```

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

```
Switch OS Image 1 ...
Un-Protected 27 sectors
Erasing Flash..... done
Writing to Flash.....done
Protected 27 sectors
```

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

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

14. Press the Escape key (<Esc>) to re-display the Boot Management menu.
Select **4** to exit and boot the new image.

Recovering a Failed Boot Image

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

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
 - Speed: 9600 bps
 - Data Bits: 8
 - Stop Bits: 1
 - Parity: None
 - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing <Shift B> while the Memory Test is in progress and the dots are being displayed.
4. Select **4** for **Xmodem download**. You will see the following display:

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

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

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

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

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

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

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

Boot image recovery is complete.

Chapter 7. Maintenance Commands

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

Dump information contains internal switch state data that is written to flash memory on the SI4093 10Gb System Interconnect Module after any one of the following occurs:

- The watchdog timer forces a switch reset. The purpose of the watchdog timer is to reboot the switch if the switch software freezes.
- The switch detects a hardware or software problem that requires a reboot.

To use the maintenance commands, you must be logged in to the switch as the administrator.

Table 166. General Maintenance Commands

Command Syntax and Usage
<pre>show flash-dump-uuencode</pre> <p>Displays dump information in uuencoded format. For details, see page 231.</p> <p>Command mode: All</p>
<pre>copy flash-dump tftp</pre> <p>Saves the system dump information via TFTP. For details, see page 232.</p> <p>Command mode: All except User EXEC</p>
<pre>copy flash-dump ftp</pre> <p>Saves the system dump information via FTP. For details, see page 232.</p> <p>Command mode: All except User EXEC</p>
<pre>clear flash-dump</pre> <p>Clears dump information from flash memory.</p> <p>Command mode: All except User EXEC</p>
<pre>show tech-support [l2 l3 link port]</pre> <p>Dumps all SI4093 information, statistics, and configuration. You can log the output (<code>tsdmp</code>) into a file. To filter the information, use the following options:</p> <ul style="list-style-type: none">– <code>l2</code> displays only Layer 2-related information– <code>l3</code> displays only Layer 3-related information– <code>link</code> displays only link status-related information– <code>port</code> displays only port-related information <p>Command mode: All except User EXEC</p>

Table 166. General Maintenance Commands

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

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 167. FDB Manipulation Commands

Command Syntax and Usage
<pre>show mac-address-table address <MAC address></pre> <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"> – xx:xx:xx:xx:xx:xx (such as 08:00:20:12:34:56) – xxxxxxxxxxxxxx (such as 080020123456) <p>Command mode: All except User EXEC</p>
<pre>show mac-address-table interface port <port number or alias></pre> <p>Displays all FDB entries for a particular port.</p> <p>Command mode: All except User EXEC</p>
<pre>show mac-address-table portchannel <trunk group number></pre> <p>Displays all FDB entries for a particular trunk group.</p> <p>Command mode: All</p>
<pre>show mac-address-table vlan <VLAN number></pre> <p>Displays all FDB entries on a single VLAN.</p> <p>Command mode: All except User EXEC</p>
<pre>show mac-address-table state {forward trunk unknown}</pre> <p>Displays all FDB entries of a particular state.</p> <p>Command mode: All except User EXEC</p>
<pre>show mac-address-table static</pre> <p>Displays static entries in the FDB.</p> <p>Command mode: All except User EXEC</p>
<pre>no mac-address-table static {<MAC address> all}</pre> <p>Removes static FDB entries.</p> <p>Command mode: All except User EXEC</p>
<pre>clear mac-address-table static</pre> <p>Clears all static entries from the Forwarding Database.</p> <p>Command mode: All except User EXEC</p>
<pre>clear mac-address-table</pre> <p>Clears the entire Forwarding Database from switch memory.</p> <p>Command mode: All except User EXEC</p>

Debugging Commands

The Miscellaneous Debug Commands display trace buffer information about events that can be helpful in understanding switch operation. You can view the following information using the debug commands:

- Events traced by the Management Processor (MP)
- Events traced to a buffer area when a reset occurs

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

If the switch resets for any reason, the MP trace buffer is saved into the snap trace buffer area. The output from these commands can be interpreted by Technical Support personnel.

Table 168. Miscellaneous Debug Commands

Command Syntax and Usage
<code>debug debug-flags</code> This command sets the flags that are used for debugging purposes. Command mode: All except User EXEC
<code>debug mp-trace</code> 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
<code>debug dumpbt</code> Displays the backtrace log. Command mode: All except User EXEC
<code>debug mp-snap</code> 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
<code>clear flash-config</code> Deletes all flash configuration blocks. Command mode: All except User EXEC

Table 168. Miscellaneous Debug Commands

Command Syntax and Usage
<pre>[no] debug lacp packet [receive transmit both] [port <port numbers>]</pre> <p>Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP.</p> <p>The following parameters are available:</p> <ul style="list-style-type: none">– <code>receive</code> filters only LACP packets received– <code>transmit</code> filters only LACP packets sent– <code>both</code> filters LACP packets either sent or received– <code>port</code> filters LACP packets sent/received on specific ports <p>By default, LACP debugging is disabled.</p> <p>Command mode: Privileged EXEC</p>

LLDP Cache Manipulation

[Table 169](#) describes the LLDP cache manipulation commands.

Table 169. LLDP Cache Manipulation commands

Command Syntax and Usage
<pre>show lldp port <port alias or number></pre> <p>Displays Link Layer Discovery Protocol (LLDP) port information.</p> <p>Command mode: All</p>
<pre>show lldp receive</pre> <p>Displays information about the LLDP receive state machine.</p> <p>Command mode: All</p>
<pre>show lldp transmit</pre> <p>Displays information about the LLDP transmit state machine.</p> <p>Command mode: All</p>
<pre>show lldp remote-device [<I-256> detail]</pre> <p>Displays information received from LLDP -capable devices. For more information, see page 31.</p> <p>Command mode: All</p>
<pre>show lldp</pre> <p>Displays all LLDP information.</p> <p>Command mode: All</p>
<pre>clear lldp</pre> <p>Clears the LLDP cache.</p> <p>Command mode: All</p>

Uencode Flash Dump

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

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

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

Note: Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see [page 233](#).

To access dump information, enter:

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

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

```
No FLASH dump available.
```

TFTP or FTP System Dump Put

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

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

```
Router# copy flash-dump tftp <server filename>
```

You are prompted for the TFTP server IP address or hostname, and the *filename* of the target dump file.

To save dump information via FTP, enter:

```
Router# copy flash-dump ftp <server filename>
```

You are prompted for the FTP server IP address or hostname, your *username* and *password*, and the *filename* of the target dump file.

Clearing Dump Information

To clear dump information from flash memory, enter:

```
Router# clear flash-dump
```

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

```
FLASH dump region cleared.
```

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

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

Unscheduled System Dumps

If there is an unscheduled system dump to flash memory, the following message is displayed when you log on to the switch:

```
Note: A system dump exists in FLASH. The dump was saved
      at 13:43:22 Wednesday January 30, 2010. Use show flash-dump
      uuencode to
      extract the dump for analysis and clear flash-dump to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Appendix A. IBM Networking OS System Log Messages

The SI4093 10Gb System Interconnect Module (SI4093) uses the following syntax when outputting system log (syslog) messages:

<Time stamp><Log Label>IBMOS<Thread ID> : <Message>

The following parameters are used:

- *<Timestamp>*

The time of the message event is displayed in the following format:

<month (3 characters)> <day> <hour (1-24)> : <minute> : <second>

For example: Aug 19 14 : 20 : 30

- *<Log Label>*

The following types of log messages are recorded: LOG_CRIT, LOG_WARNING, LOG_ALERT, LOG_ERR, LOG_NOTICE, and LOG_INFO

- *<Thread ID>*

This is the software thread that reports the log message. For example:

stg, ip, console, telnet, vrrp, system, web server, ssh, bgp

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only the *<Thread ID>* and *<Message>* are shown. The messages are sorted by *<Log Label>*.

Where the *<Thread ID>* is listed as *mgmt*, one of the following may be shown: console, telnet, web server, or ssh.

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
BGP	session with <IP address> failed (bad event:<event>)
BGP	session with <IP address> failed <reason> Reasons: <ul style="list-style-type: none"> • Connect Retry Expire • Holdtime Expire • Invalid • Keepalive Expire • Receive KEEPALIVE • Receive NOTIFICATION • Receive OPEN • Receive UPDATE • Start • Stop • Transport Conn Closed • Transport Conn Failed • Transport Conn Open • Transport Fatal Error
HOTLINKS	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
IP	cannot contact default gateway <IP address>
IP	Route table full
MGMT	Maximum number of login failures (<threshold>) has been exceeded.
OSPF	Interface IP <IP address>, Interface State {Down Loopback Waiting P To P DR BackupDR DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down Attempt Init 2 Way ExStart Exchange Loading Full Loopback Waiting P To P DR BackupDR DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
STP	CIST new root bridge
STP	CIST topology change detected
STP	Fast Forward port <port> active, putting port into forwarding state
STP	New preferred Fast Uplink port <port> active for STG <STG>, {restarting canceling} timer
STP	own BPDU received from port <port>
STP	Port <port>, putting port into blocking state
STP	Preferred STG <STG> Fast Uplink port has gone down. Putting secondary Fast Uplink port <port> into forwarding

Thread	LOG_ALERT Message (continued)
STP	Setting STG <STG> Fast Uplink primary port <port> forwarding and backup port <port> blocking
STP	STG <STG> preferred Fast Uplink port <port> active. Waiting <seconds> seconds before switching from port <port>
STP	STG <STG> root port <port> has gone down. Putting backup Fast Uplink port <port> into forwarding
STP	STG <STG>, new root bridge
STP	STG <STG>, topology change detected
SYSTEM	LACP trunk <trunk ID> and <trunk ID> formed with admin key <key>
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
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
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
NTP	unable to listen to NTP port
STP	Cannot set "{Hello Time Max Age Forward Delay Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]
SYSTEM	Not enough memory!

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user <i><username></i> .
	System log cleared via SNMP.
HOTLINKS	"Error" is set to "{Active Standby}"
HOTLINKS	"Learning" is set to "{Active Standby}"
HOTLINKS	"None" is set to "{Active Standby}"
HOTLINKS	"Side Max" is set to "{Active Standby}"
HOTLINKS	has no "{Side Max None Learning Error}" interface
MGMT	<i>/* Config changes at <time> by <username> */ <config diff> /* Done */</i>
MGMT	<i><username></i> ejected from BBI
MGMT	<i><username></i> (<i><user type></i>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	<i><username></i> (<i><user type></i>) login {on Console from host <i><IP address></i> }
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <i><hostname></i> via browser}, filename too long to be displayed, software version <i><version></i>
MGMT	boot kernel downloaded from host <i><hostname></i> , file' <i><filename></i> ', software version <i><version></i>
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 <i><hostname></i> : <i><filename></i>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting

Thread	LOG_INFO Message (continued)
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	image1 2 download completed. Now writing to flash.
MGMT	image1 2 downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	image1 2 downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Incorrect image being loaded
MGMT	Invalid diff track address. Continuing with apply()
MGMT	Invalid image being loaded for this switch type
MGMT	invalid image download completed. Now writing to flash.
MGMT	invalid image downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	invalid image downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	New config set
MGMT	new configuration applied [from BBI EM SCP SNMP Stacking Master]
MGMT	new configuration saved from {BBI ISCLI SNMP}
MGMT	scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	scp<username>(<user type>) login {on Console from host <IP address>}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <hostname> via browser}, filename too long to be displayed, software version <version>
MGMT	SP boot kernel downloaded from host <hostname>, file '<filename>', software version <version>
MGMT	Starting Firmware download for {invalid image image1 image2 boot kernel undefined SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <hostname>:<filename>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.

Thread	LOG_INFO Message (continued)
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
SSH	scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
SSH	scp<username>(<user type>) login {on Console from host <IP address>}
SSH	server key autogen {starts completes}
SSH	Wrong config file type
SYSTEM	booted version <version> from Flash image <image>, {active backup factory} config block

LOG_NOTICE

Thread	LOG_NOTICE Message
	ARP table is full.
	Current config successfully tftp'd <filename> from <hostname>
	Current config successfully tftp'd to <hostname>: <filename>
	Port <port> mode is changed to full duplex for 1000 Mbps operation.
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
MGMT	FLASH Dump cleared from BBI

Thread	LOG_NOTICE Message (continued)
MGMT	New config set
MGMT	packet-buffer statistics cleared
MGMT	PANIC command from CLI
MGMT	PASSWORD FIX-UP MODE IN USE
MGMT	Password for {oper operator} changed by {SNMP user <username>}, notifying admin to save.
MGMT	QSFP: Port <port> changed to {10G 40G}, from {BBI SNMP CLI}.
MGMT	RADIUS server timeouts
MGMT	RADIUS: authentication timeout. Retrying...
MGMT	RADIUS: failed to contact {primary secondary} server
MGMT	RADIUS: No configured RADIUS server
MGMT	RADIUS: trying alternate server...
MGMT	scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}
MGMT	scp<username>(<user type>) login {on Console from host <IP address>}
MGMT	second syslog host changed to {this host <IP address>}
MGMT	selectable [boot] mode changed
MGMT	STP BPDU statistics cleared
MGMT	switch reset from CLI
MGMT	syslog host changed to {this host <IP address>}
MGMT	System clock set to <time>.
MGMT	System date set to <date>.
MGMT	Terminating BBI connection from host <IP address>
MGMT	User <username> deleted by {SNMP user <username>}.
MGMT	User <username> is {deleted disabled} and will be ejected by {SNMP user <username>}
MGMT	User {oper operator} is disabled and will be ejected by {SNMP user <username>}.
MGMT	Wrong config file type
NTP	System clock updated
OSPF	Neighbor Router ID <router ID>, Neighbor State {Down Loopback Waiting P To P DR BackupDR DR Other Attempt Init 2 Way ExStart Exchange Loading Full}

Thread	LOG_NOTICE Message (continued)		
SERVER	link {down up} on port <port>		
SSH	(remote disconnect msg)		
SSH	<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}		
SSH	<username>(<user type>) login {on Console from host <IP address>}		
SSH	Error in setting the new config		
SSH	Failed login attempt via SSH		
SSH	New config set		
SSH	scp<username>(<user type>) {logout ejected idle timeout connection closed} from {Console Telnet/SSH}		
SSH	scp<username>(<user type>) login {on Console from host <IP address>}		
SSH	Wrong config file type		
SYSTEM	Change fiber GIG port <port> mode to full duplex		
SYSTEM	Change fiber GIG port <port> speed to 1000		
SYSTEM	Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN>		
SYSTEM	Enable auto negotiation for copper GIG port: <port>		
SYSTEM	I2C device <ID> <description> set to access state <state> [from CLI]		
SYSTEM	Port <port> disabled		
SYSTEM	Port <port> disabled due to reason code <reason code>		
SYSTEM	rebooted (<reason>)[, administrator logged in] Reason: <table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top;"> <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 </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • 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 </td> </tr> </table>	<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 	<ul style="list-style-type: none"> • 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
<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 	<ul style="list-style-type: none"> • 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 		

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

LOG_WARNING

Thread	LOG_WARNING Message
CFG	Authentication should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <i><interface></i> .
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <i><interface></i> .
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
NTP	cannot contact [primary secondary] NTP server <i><IP address></i>
SYSTEM	I2C device <i><ID></i> <i><description></i> set to access state <i><state></i> [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 IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the *IBM Documentation CD* that comes with your system.
- Go to the IBM support website at <http://www.ibm.com/systems/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and pre-installed software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, ReadMe files, and Help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/systems/support/> and follow the instructions. Also, some documents are available through the IBM Publications Center at <http://www.ibm.com/shop/publications/order/>.

Getting help and information on the World Wide Web

On the World Wide Web, the IBM website has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x[®] and xSeries[®] information is <http://www.ibm.com/systems/x/>. The address for IBM BladeCenter information is <http://www.ibm.com/systems/bladecenter/>. The address for IBM IntelliStation[®] information is <http://www.ibm.com/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/systems/support/>.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and x Series servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld/> and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see <http://www.ibm.com/planetwide/>. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Index

Numerics

- 802.1p
 - and ETS 193
 - configuration 165
 - DCBX PFC information 50
 - information 53
 - PFC configuration 194
 - Priority Group mapping 53
 - priority level 156
 - IPv6 160
 - priority value 167
 - re-marking the value (IPv6) 163

A

- abbreviating commands (CLI) 6
- access control
 - switch 138
 - user 140
- Access Control List (see ACL) 41
- ACL
 - add group 149
 - configuration 155
 - delete 207
 - Ethernet matching criteria 157
 - filtering criteria 156
 - groups 155
 - information 41, 42
 - IPv4 matching criteria 158
 - IPv6 160
 - list of FIPS ACLs 55, 56
 - metering configuration 164
 - Packet Format matching criteria 160
 - port ACL configuration 149
 - port configuration commands 149
 - QoS parameters 149
 - re-marking 165
 - re-marking (IPv6) 163, 167
 - remove group 149
 - statistics 97, 98
 - TCP matching criteria 159
 - UDP matching criteria 159
- active
 - configuration block 108, 217
 - switch configuration
 - ptcfg 203
 - restoring 204
 - saving and loading 204
- administrator account 7

B

- backup configuration block 217
- bandwidth allocation, Priority Groups 193
- boot

- options 211 to 222
- Boot Management menu 220

C

- capture dump information to a file 231
- CEE
 - configuration 192
 - information 46
- Cisco Ether Channel 175
- clear
 - ACL statistics 97
 - all defined management networks 139
 - all IP statistics 74
 - all IPv4 statistics 73, 74
 - DNS statistics 73
 - dump information 233
 - FCoE statistics 99
 - LACP statistics 69
 - statistics for specific ports 60
 - statistics on a specific trunk group 68
 - TCP statistics 73
 - UDP statistics 73
- commands
 - abbreviations 6
 - conventions used in this manual xii
 - help with 4
 - shortcuts 6
 - tab completion 6
- configuration
 - commands 107 to 204
 - default gateway interval, for health checks 186
 - default gateway IP address 186
 - dump command 202
 - failover 180
 - flow control 147, 151
 - port link speed 147
 - port trunking 175
 - save changes 108
 - SNMP 125
 - switch IP address 184
 - TACACS+ 118
 - VLAN default (PVID) 144
 - VLAN IP interface 184
 - VLAN tagging 144
- configuration block
 - active 217
 - backup 217
 - factory 217
 - selection 217
- Control Plane Protection, configuration 153
- Converged Enhanced Ethernet (see CEE) 46
- COPP, configuration 153
- CPU use
 - history 96

statistics 93, 96

D

daylight saving time 109

DCB Capability Exchange Protocol (see DCBX) 46

DCBX

Application Protocol information 51

configuration 195

control information 47

ETS information 48

feature information 48

information 46

PFC information 50

debugging 225

default gateway

information 36

interval, for health checks 186

IPv6 189

default password 7

delete

ACL statistics 97

all defined management networks 139

all IP statistics 74

all IPv4 statistics 73, 74

DNS statistics 73

dump information 233

LACP statistics 69

statistics for specific ports 60

statistics on a specific trunk group 68

TCP statistics 73

UDP statistics 73

DHCP

and Netboot configuration 212

binding table information 40

disconnect idle timeout 8

downloading software 214

DSCP

disable for in-profile traffic 166

disable for out-profile traffic 166

re-mark for in-profile traffic 168

set value of in-profile packets 166

set value of out-profile packets 166

dump

configuration command 202

maintenance 225

duplex mode

interface status 9

link status 42

E

ECN (Explicit Congestion Notification) 153

Enhanced Transmission Selection (see ETS) 53

ENode 198

Error Disable and Recovery

port 146

system 112

EtherChannel, and port trunking 175

ETS

configuration 193

information 46, 48, 53

Priority Group configuration 193

Explicit Congestion Notification (ECN) 153

F

factory configuration block 217

failover

configuration 180

Layer 2 configuration 180

Layer 2 information 25, 29

manual monitor port configuration 181

trigger configuration 180

FCF port 198

FCoE

configuration 197

FIPS port configuration 198

forwarding 198

information 55

Initialization Protocol (see FIP) 198

statistics 99

FDB

configuration 169

configuring static entries 170

information 26

learning 145

maintenance 225, 227

troubleshooting 225, 227

Fiber Channel Initialization Protocol (see FIP) 55

Fibre Channel over Ethernet (see FCoE) 55

FIP

Snooping (see FIPS) 198

snooping information 55

FIPS

list of ACLs 55

port configuration 198

flow control

configuring 147, 151

configuring for port link 147

configuring management port 151

information 9, 42

pause packets 65, 66

priority (see PFC) 50

Forwarding Database (see FDB) 26

forwarding state (FWD) 27, 34

FWD (port state) 27

G

getting help 249

gtcfg (TFTP load command) 204

H

hardware service and support 254

- health checks
 - default gateway interval, retries 186
 - retry, number of failed health checks 186
- help
 - getting 249
 - online 4

I

- IBM support line 253
- idle timeout, setting 8
- image
 - downloading 214
 - software, selecting 215
- Information Commands 9 to 57
- IP address
 - configuring default gateway 186
- IP forwarding
 - information 36
- IP Information 36, 40
- IP interfaces
 - configuring address 184
 - configuring VLANs 184
 - information 36
- IP network filter configuration 187
- IP statistics 74
- IPv6
 - ACL configuration 160
 - default gateway configuration 189
 - interface information 39
 - Neighbor Discovery
 - cache information 37
 - cache information commands 37
 - prefix configuration 190
 - prefix information 38
 - Path MTU
 - configuration 189
 - information 39
 - re-mark configuration 163
 - re-marking
 - configuration 167
 - in-profile configuration 168
- ISCLI command modes 2

L

- LACP
 - admin key
 - add to Manual Monitor Control 182
 - add to Manual Monitor Port 181
 - remove from Manual Monitor Control 182
 - remove from Manual Monitor Port 181
 - aggregator information 28
 - and trunk hash configuration 176
 - configuration 178
 - information 28
 - port configuration 179
 - port status information 28

- show trunk groups 25
- statistics 69, 70
- Layer 2 commands 25
- Layer 3 commands 36
- LDAP server configuration 121
- Lightweight Directory Access Protocol (see LDAP) 121
- Link Aggregation Control Protocol (see LACP) 25
- Link Layer Discovery Protocol (see LLDP) 30
- link speed, configuring 147
- link status 9
 - command 42
 - duplex mode 9, 42
 - information 42
 - port speed 9, 42
- linkt (SNMP option) 126
- LLDP
 - cache manipulation commands 230
 - configuration 170
 - disable 171
 - enable 171
 - information 30
 - packets received 85
 - PDUs logged 90
 - remote device information 31
 - statistics 69, 71
 - TLV configuration 173
- log, syslog messaging options 114

M

- MAC address
 - display 10
 - FDB information 26
 - FDB maintenance 227
 - switch management processor 21
- Maintenance commands 225
- Management Processor (see MP) 10
- manual style conventions xii
- meter
 - ACL
 - configuring 164
 - current parameters 165
 - delete 165
 - log, configuring 165
 - readiness 220
- Miscellaneous Debug commands 228
- MP
 - display MAC address 10, 21
 - packet statistics 81
 - snap trace buffer 228
 - statistics 80
 - trace buffer 228
- MTU 189

N

- Neighbor Discovery
 - prefix 190

Neighbor Discovery prefix 190
notice 110
NTP synchronization 124

O

OAM
 information 33
 statistics 60, 69, 72
online help 4
Operations commands 205
operations-level
 port commands 206

P

passwords 7
 administrator account 7
 changing 140
 default 7
 user account 7
Path MTU 189
PFC configuration 194
ping 4
port
 ACL configuration 149
 configuration 144
 disabling temporarily 147
 Error Disable and Recovery 146
 failover manual monitor configuration 181
 FIPS configuration 198
 information 43
 LACP
 configuration 179
 status information 28
 link configuration 147
 link speed, configuring 147
 management, configuring 151
 membership of the VLAN 25, 35
 number 42
 reference 27
 speed 9, 42
 state information 27
 telnet 137
 TFTP 138
 trunking
 configuration 175
 description 175
 VLAN ID 9, 43
port ECN configuration 150
port WRED configuration 150
Priority Flow Control 194
Priority Groups
 802.1p mapping to 53
 configuration 193
 information 48
Protected Mode 208
ptcfg (TFTP save command) 203

PVID (port VLAN ID) 9, 43

Q

QoS
 ACL parameters 149
 configuration 149, 153
 control plane protection 153
 information 41

R

RADIUS server
 configuration commands 116
 current parameters 117
 packets logged 90
 primary 116
 shared secret 116
receive flow control 147, 151
reference ports 27
re-mark
 ACL
 configuration 165
 parameters 42
 in-profile
 configuration 166
 IPv6 ACL 163
 configuration 167
 in-profile configuration 168
 out-of-profile
 configuration 166
retries
 health checks for default gateway 186
 radius server 116

S

save (global command) 108
secret, RADIUS server 116
Secure Shell 115
service and support 254
shortcuts (CLI) 6
SLP
 configuration 200
snap trace buffer 228
SNMP
 configuration
 commands 125
 current 126
 link traps 126
 location 125
 read community string 125
 source interface for traps 126
 system authentication trap 126
 system contact 125
 timeout 126
 trap host server 126
 version 128

- write community string 126
 - options 125
 - statistics 100
- SNMPv3
 - configuration
 - access rights 127
 - commands 127
 - community table 127, 133
 - destination 128
 - display 128
 - group 127, 132
 - MIB views 127
 - Notify table 136
 - parameters 128
 - target address table 134
 - target parameters 135
 - user access 131
 - user security 129
 - USM 127, 129
 - version 128
 - view 130
 - information 20
 - access 16
 - commands 13
 - community table 17
 - group 16
 - Notify table 19
 - target address table 17
 - target parameters table 19
 - USM user table 14
 - View Table 15
- software
 - image 214
 - image file and version 10, 21
 - service and support 253
 - upgrade recovery 220
- SPAR. See Switch Partition.
- statistics
 - ACL 97
 - bridging 61
 - commands 59 to 106
 - CPU 93
 - DNS 76
 - ethernet 62
 - FCoE 99
 - interface 65
 - interface protocol 67
 - IPv4 74
 - LACP 70
 - Layer 2 69
 - Layer 3 73
 - link 67
 - LLDP 71
 - logged packet 89
 - management processor 80
 - NTP 104
 - OAM 72
 - port 60

- SNMP 100
- TCP 77, 92
- trunk group 68
- UDP 78, 93
- STP
 - and trunk groups 34
- support
 - line 253
 - Web site 253
- switch
 - name and location 10, 21
 - resetting 218
- Switch Partition (SPAR)
 - configuration 199
- Switch Partition (SPAR)
 - configuration 3
- system
 - date and time 10, 21
 - information 10, 21
- System Error Disable and Recovery 112

T

- tab completion (CLI) 6
- TACACS+ 118
- TCP statistics 77, 92
- technical assistance 249
- telephone assistance 253
- telephone numbers 255
- telnet
 - configuring switches using 202
 - controlling access 137
 - port 137
 - radius server 116, 121
- text conventions xii
- TFTP 214
 - port 138
 - PUT and GET commands 203
 - server 203
- timeout
 - idle connection 8
 - radius server 116
- TLV 173
- trace buffer 228
- traceroute 5
- transceiver status 45
- transmit flow control 147, 151
- Trunk group information 33
- trunk hash algorithm 176
- typographic conventions, manual xii

U

- UCB statistics 93
- UDLD
 - configuration 148
 - information 32
 - statistics 84, 89

- UDP statistics 78
- unknown (UNK) port state 27
- Unscheduled System Dump 234
- upgrade
 - recover from failure 220
 - switch software 214
- user access control configuration 140
- user account 7
- Uuencode Flash Dump 231

V

VLAN

- information 35
- name 25
- Number 35
- port membership 25, 35
- setting default number (PVID) 144
- tagging 43
 - port configuration 144
 - port use of 9

W

- watchdog timer 225
- Web site
 - ordering publications 251
 - support 253
 - telephone support numbers 254
- Weighted Random Early Detection (WRED) 153
- WRED (Weighted Random Early Detection) 153



Part Number: 00AY527

Printed in USA

(IP) P/N: 00AY527