IBM Flex System SI4093 10Gb System Interconnect Module (SIM)

ISCLI—Industry Standard CLI Command Reference

for IBM Networking OS 7.8

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 (June 2014)

IBM Flex System Fabric SI4093 System Interconnect Module ISCLI Command Reference

Contents

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 SI4093 10Gb System Interconnect Module (SIM). 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, o 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`	This type is used for names of commands, files, and directories used within the text. For example: View the `readme.txt` file. It also depicts on-screen computer output and prompts.
`bold fixed-width text`	This bold type appears in command examples. It shows text that must be typed in exactly as shown. For example: `show sys-info`
bold body text	This bold type indicates objects such as window names, dialog box names, and icons, as well as user interface objects such as buttons, and tabs.
italicized body text	This italicized type indicates book titles, special terms, or words to be emphasized.

angle brackets < >	Indicate a variable to enter based on the description inside the brackets. Do not type the brackets when entering the command.
	
	Example: If the command syntax is
	`ping <`*IP address*`>`
	
	you enter
	`ping 192.32.10.12`

braces { }	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show portchannel {<`*1-128*`>|hash|information}` you enter: **`show`** `portchannel <`*1-128*`>` or show `portchannel` hash or show `portchannel` information

Table 1. Typographic Conventions

Typeface or Symbol	Meaning
brackets [ ]	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show interface ip` **[**<*125-4*>**]** you enter `show interface ip` or `show interface ip` <*125-4*>
vertical line |	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show portchannel` {<*1-128*>|`hash`|`information`} you must enter: **show** `portchannel` <*1-64*> or show `portchannel` hash or show `portchannel` information

Chapter 1. ISCLI Basics

Your SI4093 10Gb System Interconnect Module (SIM) (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: `exit` or `logout`
Privileged EXEC `Router#`	Enter Privileged EXEC mode, from User EXEC mode: `enable` Exit to User EXEC mode: `disable` Quit ISCLI: `exit` or `logout`
Global Configuration `Router(config)#`	Enter Global Configuration mode, from Privileged EXEC mode: `configure terminal` Exit to Privileged EXEC: `end` or `exit`
Interface IP `Router(config-ip-if)#`	Enter Interface IP Configuration mode, from Global Configuration mode: `interface ip` <*interface number*> Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`

Table 1. ISCLI Command Modes (continued)

Command Mode/Prompt	Command used to enter or exit
Interface Port `Router(config-if)#`	Enter Port Configuration mode, from Global Configuration mode: `interface port <`*port number or alias*`>` Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`
Interface PortChannel `Router(config-PortChannel)#`	Enter PortChannel (trunk group) Configuration mode, from Global Configuration mode: `interface portchannel {<`*trunk number*`>|lacp <`*key*`>}` Exit to Privileged EXEC mode: `exit` Exit to Global Configuration mode: `end`
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`
VSI Database `SI4093(conf-vsidb)#`	Enter Virtual Station Interface Database Configuration mode, from Global Configuration mode: `virt evb vsidb <`*VSIDB_number*`>` Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
EVB Profile `SI4093(conf-evbprof)#`	Enter Edge Virtual Bridging Profile Configuration mode, from Global Configuration mode: `virt evb profile <`*1-16*`>` Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
UFP Virtual Port Configuration `SI4093(config_ufp_vport)#`	Enter Unified Fabric Port Virtual Port Configuration mode, from Global Configuration mode: `ufp port <`*port no.*`> vport <`*1-4*`>` Exit to Global Configuration mode: `exit` Exit to Privileged EXEC mode: `end`
SPAR Configuration `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`	Use this command to verify station-to-station connectivity across the network. The format is as follows: `ping` *<host name>*|*<IP address>* `[-n` *<tries (0-4294967295)>*`] [-w` *<msec delay (0-4294967295)>*`] [-l` *<length (0/32-65500/2080)>*`] [-s` *<IP source>*`] [-v` *<tos (0-255)>*`] [-f] [-t]` Where: – `-n`: Sets the number of attempts (optional). – `-w`: Sets the number of milliseconds between attempts (optional). – `-l`: Sets the ping request payload size (optional). – `-s`: Sets the IP source address for the IP packet (optional). – `-v`: Sets the Type Of Service bits in the IP header. – `-f`: Sets the *don't fragment* bit in the IP header (only for IPv4 addresses). – `-t`: Pings continuously (same as `-n 0`). Where the *IP address* or *hostname* specify the target device. Use of a hostname requires DNS parameters to be configured on the switch. *Tries* (optional) is the number of attempts (1-32), and *msec delay* (optional) is the number of milliseconds between attempts.

Table 2. Description of Global Commands (continued)

Command	Action
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: `traceroute` {<*hostname*>|<*IP address*>} [<*max-hops (1-32)*> [<*msec delay*>]] `traceroute` <*hostname*>|<*IP address*> [<*max-hops (1-32)*> [<*msec-delay (1-4294967295)*>]] Where *hostname/IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *msec-delay* (optional) is the number of milliseconds to wait for the response. As with `ping`, the DNS parameters must be configured if specifying hostnames.
`telnet`	This command is used to form a Telnet session between the switch and another network device. The format is as follows: `telnet` {<*hostname*>|<*IP address*>} [<*port*>] Where *IP address* or *hostname* specifies the target station. Use of a hostname requires DNS parameters to be configured on the switch. *Port* is the logical Telnet port or service number.
`show history`	This command displays the last ten issued commands.
`show who`	Displays a list of users who are currently logged in.
`show line`	Displays a list of users who are currently logged in, in table format.

Command Line Interface Shortcuts

The following shortcuts allow you to enter commands quickly and easily.

CLI List and Range Inputs

For VLAN and port commands that allow an individual item to be selected from within a numeric range, lists and ranges of items can now be specified. For example, the `vlan` command permits the following options:

`# vlan 1,3,4095`	*(access VLANs 1, 3, and 4095)*
`# vlan 1-20`	*(access VLANs 1 through 20)*
`# vlan 1-5,90-99,4090-4095`	*(access multiple ranges)*
`# vlan 1-5,19,20,4090-4095`	*(access a mix of lists and ranges)*

The numbers in a range must be separated by a dash: *<start of range>-<end of range>*

Multiple ranges or list items are permitted using a comma: *<range or item 1>*, *<range or item 2>*

Do not use spaces within list and range specifications.

Ranges can also be used to apply the same command option to multiple items. For example, to access multiple ports with one command:

`# interface port 1-4`	*(Access ports 1 though 4)*

Command Abbreviation

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

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

or

```
Router(config)# sp stp 2 br h 2
```

Tab Completion

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

User Access Levels

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the 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 (SIM), including the ability to change both the user and administrator passwords.	`admin`

Note: With the exception of the “admin” user, access to each user level can be disabled by setting the password to an empty value.

Idle Timeout

By default, the switch will disconnect your Telnet session after ten minutes of inactivity. This function is controlled by the following command, which can be set from 1 to 60 minutes, or disabled when set to 0:

`system idle <`*0-60*`>`

Command mode: Global Configuration

Chapter 2. Information Commands

You can view configuration information for the switch in both the user and administrator command modes. This chapter discusses how to use the command line interface to display switch information.

Table 4. Information Commands

Command Syntax and Usage
`show interface status` <*port alias or number*> Displays configuration information about the selected port(s), including: – Port alias and number – Port speed – Duplex mode (half, full, or auto) – Flow control for transmit and receive (no, yes, or both) – Link status (up, down, or disabled) For details, see page 46. **Command mode:** All
`show interface trunk` <*port alias or number*> Displays port status information, including: – Port alias and number – Whether the port uses VLAN Tagging or not – Port VLAN ID (PVID) – Port name – VLAN membership – FDB Learning status – Flooding status For details, see page 47. **Command mode:** All
`show interface transceiver` Displays the status of the port transceiver module on each external port. For details, see page 48. **Command mode:** All
`show information-dump` Dumps all switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

System Information

The information provided by each command option is briefly described in Table 5 on page 10, with pointers to where detailed information can be found.

Table 5. System Information Commands

Command Syntax and Usage
`show sys-info` Displays system information, including: – 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 For details, see page 21. **Command mode:** All
`show logging [severity <0-7>] [reverse]` Displays the current syslog configuration, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 23. **Command mode:** All
`show access user` Displays configured user names and their status. **Command mode:** Privileged EXEC

CLI Display Information

These commands allow you to display information about the number of lines per screen displayed in the CLI.

Table 6. CLI Display Information Options

Command Syntax and Usage
`show terminal-length` Displays the number of lines per screen displayed in the CLI for the current session. A value of 0 means paging is disabled. **Command mode:** All
`show line console length` Displays the current `line console length` setting. For details, see page 125. **Command mode:** All
`show line vty length` Displays the current `line vty length` setting. For details, see page 125. **Command mode:** All

Error Disable and Recovery Information

These commands allow you to display information about the Error Disable and Recovery feature for interface ports.

Table 7. Error Disable Information Commands

Command Syntax and Usage
`show errdisable recovery` Displays a list ports with their Error Recovery status. **Command mode:** All
`show errdisable timers` Displays a list of active recovery timers, if applicable. **Command mode:** All
`show errdisable information` Displays all Error Disable and Recovery information. **Command mode:** All

SNMPv3 System Information

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

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

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

Table 8. SNMPv3 Commands

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

Table 8. SNMPv3 Commands (continued)

Command Syntax and Usage
`show snmp-server v3 notify` Displays the Notify table information. To view a sample, see page 19. **Command mode:** All
`show snmp-server v3` Displays all the SNMPv3 information. To view a sample, see page 20. **Command mode:** All

SNMPv3 USM User Table Information

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

```
show snmp-server v3 user
```

Command mode: All

The USM user table contains the following information:

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

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

Table 9. USM User Table Information Parameters

Field	Description
User Name	This is a string that represents the name of the user that you can use to access the switch.
Protocol	This indicates whether messages sent on behalf of this user are protected from disclosure using a privacy protocol. 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
usm          adminshaaes                     admingrp
```

Table 12. SNMPv3 Group Table Information Parameters

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

SNMPv3 Community Table Information

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

```
show snmp-server v3 community
```

Command mode: All

```
Index      Name       User Name           Tag
---------- ---------- ------------------- ----------
trap1      public     v1v2only            v1v2trap
```

Table 13. SNMPv3 Community Table Information Parameters

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

SNMPv3 Target Address Table Information

The following command displays SNMPv3 target address information:

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

Command mode: All

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

```
Name       Transport Addr  Port Taglist    Params
---------- --------------- ---- ---------- ---------------
trap1      47.81.25.66     162  v1v2trap   v1v2param
```

Table 14. SNMPv3 Target Address Table Information Parameters

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

SNMPv3 Target Parameters Table Information

The following command displays SNMPv3 target parameters information:

```
show snmp-server v3 target-parameters
```

Command mode: All

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

Table 15. SNMPv3 Target Parameters Table Information

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

SNMPv3 Notify Table Information

The following command displays the SNMPv3 Notify table:

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

Command mode: All

```
Name                Tag
------------------- -------------------
v1v2trap            v1v2trap
```

Table 16. SNMPv3 Notify Table Information

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

SNMPv3 Dump Information

The following command displays SNMPv3 information:

```
show snmp-server v3
```

Command mode: All

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

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

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

vacmSecurityToGroup Table:
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 SI4093 10Gb System Interconnect Module (SIM)

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)

MAC address: 00:00:00:00:00:00    IP (If 1) address: 0.0.0.0
Internal Management Port MAC Address: 00:00:00:00:00:ef
Internal Management Port IP Address (if 128): 9.43.95.121
External Management Port MAC Address: 00:00:00:00:00:fe
External Management Port IP Address (if 127):
WARNING:  This is UNRELEASED SOFTWARE for LAB TESTING ONLY.
          DO NOT USE IN A PRODUCTION NETWORK.

Software Version 7.9.0.19 (FLASH image2), active configuration.
Boot kernel version 7.9.0.19

Hardware Part Number        : 95Y3315
Hardware Revision           : 05
Serial Number               : Y030CM31B047
Manufacturing Date (WWYY)   : 0513



PCBA Part Number            : 00D6224
PCBA Revision               : 0
PCBA Number                 : 00
Board Revision              : 05
PLD Firmware Version        : 1.7
Temperature Warning         : 44 C (Warning  at 60 C / Recover at 55 C)
Temperature Shutdown        : 43 C (Shutdown at 65 C / Recover at 60 C)
Temperature Inlet           : 38 C
Temperature Exhaust         : 44 C
Temperature Asic Max        : 47 C (Warning at 100 C / Shutdown at 108 C)
Switch is in I/O Module Bay 1
```

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

System information includes:

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

Show Software Version Brief Information

The following command displays brief software version information:

```
show version brief
```

Command mode: All

```
Software Version 7.8.1.0 (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
`show version brief` Displays the software version number, image file, and configuration name. **Command mode:** All

Show Recent Syslog Messages

The following command displays system log messages:

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

Command mode: All

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

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

This command displays the status of the configured usernames.

Layer 2 Information

The following commands display Layer 2 information.

Table 18. Layer 2 Information Commands

Command Syntax and Usage
`show portchannel information` Displays the state of each port in the various static or LACP trunk groups. For details, see page 34. **Command mode:** All
`show vlan` Displays VLAN configuration information for all configured VLANs, including: – VLAN Number – VLAN Name – Status – Port membership of the VLAN For details, see page 36. **Command mode:** All
`show failover trigger <`*trigger number*`>` Displays Layer 2 Failover information. For details, see page 29. **Command mode:** All
`show layer2 information` Dumps all Layer 2 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

FDB Information

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

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

Table 19. FDB Information Commands

Command Syntax and Usage
`show mac-address-table address` <*MAC address*> Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56` You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456` **Command mode:** All
`show mac-address-table interface port` <*port alias or number*> Displays all FDB entries for a particular port. **Command mode:** All
`show mac-address-table vlan` <*VLAN number*> Displays all FDB entries on a single VLAN. **Command mode:** All
`show mac-address-table state {unknown|forward|trunk}` Displays all FDB entries for a particular state. **Command mode:** All
`show mac-address-table static` Displays all static MAC entries in the FDB. **Command mode:** All
`show mac-address-table configured static` Displays all configured static MAC entries in the FDB. **Command mode:** All
`show mac-address-table` Displays all entries in the Forwarding Database. **Command mode:** All For more information, see page 26.

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 277.

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
`show lacp aggregator` <*aggregator ID*> Displays detailed information about the LACP aggregator. **Command mode:** All
`show interface port` <*port alias or number*> `lacp information` Displays LACP information about the selected port. **Command mode:** All
`show lacp information` Displays a summary of LACP information. **Command mode:** All For details, see page 28.

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
`show failover trigger <trigger number>` Displays detailed information about the selected Layer 2 Failover trigger. **Command mode:** All
`show failover trigger` Displays a summary of Layer 2 Failover information. For details, see page 29. **Command mode:** All

Layer 2 Failover Information

The following command displays Layer 2 Failover information:

```
show failover trigger
```

Command mode: All

```
trunk 1
 EXT2       Operational
 EXT3       Operational

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

Trigger 2 Manual Monitor: Enabled
Trigger 2 limit: 0
Monitor State: Down
Member      Status
---------   -----------
adminkey 62
 EXT20      Failed
Control State: Auto Disabled
Member      Status
---------   -----------
Physical ports
 INTC1      Failed
Virtual  ports
 INTB1.2    Failed
 INTB2.2    Failed
 INTB3.2    Failed
 INTB4.2    Failed
 INTB5.2    Failed
 INTB6.2    Failed
 INTB7.2    Failed
 INTB8.2    Failed
 INTB9.2    Failed
 INTB10.2   Failed
 INTB11.2   Failed
...
```

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

LLDP Information

The following commands display LLDP information.

Table 22. LLDP Information Commands

Command Syntax and Usage
`show lldp port` Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
`show lldp receive` Displays information about the LLDP receive state machine. **Command mode:** All
`show lldp transmit` Displays information about the LLDP transmit state machine. **Command mode:** All
`show lldp remote-device [<1-256>|detail]` Displays information received from LLDP-capable devices. To view a sample display, see page 32.
`show lldp port <1-16> tlv evb` Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information. **Command mode:** All
`show lldp information` Displays all LLDP information. **Command mode:** All

LLDP Remote Device Information

The following command displays LLDP remote device information:

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

Command mode: All

```
LLDP Remote Devices Information

LocalPort | Index | Remote Chassis ID | RemotePort | Remote System Name
----------|-------|-------------------|------------|---------------------------
     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 SI4093
10Gb System Interconnect Module (SIM), 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
`show interface port <`*port alias or number*`> udld` Displays UDLD information about the selected port. **Command mode:** All
`show udld` Displays all UDLD information. **Command mode:** All

UDLD Port Information

The following command displays UDLD information for the selected port:

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

Command mode: All

```
UDLD information on port EXT1
Port enable administrative configuration setting: Enabled
Port administrative mode: normal
Port enable operational state: link up
Port operational state: advertisement
Port bidirectional status: bidirectional
Message interval: 15
Time out interval: 5
Neighbor cache: 1 neighbor detected

   Entry #1
   Expiration time: 31 seconds
   Device Name:
   Device ID: 00:da:c0:00:04:00
   Port ID: EXT1
```

UDLD information includes the following:

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

OAM Discovery Information

Table 24. OAM Discovery Information Commands

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

OAM Port Information

The following command displays OAM information for the selected port:

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

Command mode: All

```
OAM information on port EXT1
State enabled
Mode active
Link up
Satisfied Yes
Evaluating No

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

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

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
`show vlan <VLAN number>` Displays general VLAN information.
`show vlan private-vlan [type]` Displays private VLAN information. – `type` lists only the VLAN type for each private VLAN: community, isolated or primary. **Command mode:** All
`show vlan information` Displays information about all VLANs, including: – VLAN number and name – Port membership – VLAN status (enabled or disabled) – Private VLAN status –

The following command displays VLAN information:

`show vlan <VLAN number>`

Command mode: All

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

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
- Private VLAN configuration

Layer 3 Information

Table 26. Layer 3 Information Commands

Command Syntax and Usage
`show ipv6 neighbors` Displays IPv6 Neighbor Discovery cache information. For more information options, see page 38. **Command mode**: All
`show ipv6 prefix` Displays IPv6 Neighbor Discovery prefix information. For details, see page 40. **Command mode**: All
`show ip igmp groups` Displays IGMP Information. For more IGMP information options, see page 40. **Command mode**: All
`show ipv6 mld groups` Displays Multicast Listener Discovery (MLD) information. For more MLD information options, see page 75. **Command mode**: All
`show ip vrrp information` Displays VRRP information. For details, see page 77. **Command mode:** All
`show interface ip` Displays IPv4 interface information. For details, see page 43. **Command mode:** All
`show ipv6 interface` <*interface number*> Displays IPv6 interface information. For details, see page 43. **Command mode:** All
`show ipv6 pmtu [`<*destination IPv6 address*>`]` Displays IPv6 Path MTU information. For details, see page 44. **Command mode:** All

Table 26. Layer 3 Information Commands (continued)

Command Syntax and Usage
`show ip interface brief` Displays IP `Information. For details, see page 44. IP information, includes: – IP interface information: Interface number, IP address, subnet mask, VLAN number, and operational status. – Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status – IP forwarding settings, network filter settings, route map settings **Command mode:** All
`show layer3` Dumps all Layer 3 switch information available (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands. **Command mode:** All

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
`show ipv6 neighbors find` <*IPv6 address*> Shows a single IPv6 Neighbor Discovery cache entry by IP address. **Command mode:** All
`show ipv6 neighbors interface port` <*port alias or number*> Shows IPv6 Neighbor Discovery cache entries on a single port. **Command mode:** All
`show ipv6 neighbors vlan` <*VLAN number*> Shows IPv6 Neighbor Discovery cache entries on a single VLAN. **Command mode:** All

Table 27. IPv6 Neighbor Discovery Cache Information Commands

Command Syntax and Usage
`show ipv6 neighbors static` Displays static IPv6 Neighbor Discovery cache entries. **Command mode:** All
`show ipv6 neighbors` Shows all IPv6 Neighbor Discovery cache entries. For more information, see page 39. **Command mode:** All

IPv6 Neighbor Discovery Cache Information

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

```
show ipv6 neighbors
```

Command mode: All

```
IPv6 Address               Age  Link-layer Addr   State     IF  VLAN Port
-------------------------- ---- ----------------- --------- --- ---- ----
2001:2:3:4::1              10   00:50:bf:b7:76:b0 Reachable 2   1     EXT1
fe80::250:bfff:feb7:76b0   0    00:50:bf:b7:76:b0 Stale     2   1     EXT2
```

IPv6 Neighbor Discovery Prefix Information

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

```
show ipv6 prefix
```

Command mode: All

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

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

Neighbor Discovery prefix information includes information about all configured prefixes.

IGMP Multicast Group Information

Table 28. IGMP Multicast Group Information Commands

Command Syntax and Usage
`show ip igmp snoop` Displays IGMP Snooping information. **Command mode:** All
`show ip igmp filtering` Displays current IGMP Filtering parameters. **Command mode:** All
`show ip igmp profile` <*1-16*> Displays information about the current IGMP filter. **Command mode:** All
`show ip igmp groups address` <*IP address*> Displays a single IGMP multicast group by its IP address. **Command mode:** All
`show ip igmp groups vlan` <*VLAN number*> Displays all IGMP multicast groups on a single VLAN. **Command mode:** All
`show ip igmp groups interface port` <*port alias or number*> Displays all IGMP multicast groups on a single port. **Command mode:** All

Table 28. IGMP Multicast Group Information Commands (continued)

Command Syntax and Usage
`show ip igmp groups portchannel` <*trunk number*> Displays all IGMP multicast groups on a single trunk group. **Command mode:** All
`show ip igmp groups detail` <*IP address*> Displays details about an IGMP multicast group, including source and timer information. **Command mode:** All
`show ip igmp groups` Displays information for all multicast groups. For details, see page 41. **Command mode:** All
`show ip igmp ipmcgrp` Displays information for all IPMC groups. For details, see page 42. **Command mode:** All
`show ip igmp counters` Displays IGMP counters for all VLANs. **Command mode:** All
`show ip igmp vlan` <*VLAN number*> `counter` Displays IGMP counters for a specific VLAN. **Command mode:** All

IGMP Group Information

The following command displays IGMP Group information:

```
show ip igmp groups
```

Command mode: All

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

IGMP Group information includes:

- IGMP source address
- IGMP Group address

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

IGMP Multicast Router Information

The following command displays Mrouter information:

```
show ip igmp mrouter information
```

Command mode: All

```
SrcIP              VLAN    Port       Version   Expires   MRT       QRV   QQIC

------------------ ------- -------    --------- --------  -------   ----  ----
10.1.1.1            2       EXT4       V3        4:09     128        2     125
10.1.1.5            2       EXT6       V2        4:09     125        -       -
*                   9       EXT7       V2       static     -         -       -
```

IGMP Mrouter information includes:

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

IPMC Group Information

The following command displays IGMP IPMC group information:

```
show ip igmp ipmcgrp
```

Command mode: All

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

IGMP IPMC Group information includes:

- IGMPv3 source address

- Multicast group address
- VLAN and port
- Type of IPMC group
  –

Interface Information

The following command displays interface information:

```
show interface ip
```

Command mode: All

```
Interface information:
  126:    IP6 fd55:faaf:e1ab:1022:7699:75ff:fe91:a6ef/64        , vlan 4095, up
         fe80::7699:75ff:fe91:a6ef
  128:    IP4 9.37.78.51      255.255.252.0   9.37.79.255,     vlan 4095, up
```

For each interface, the following information is displayed:
- IPv4 interface address and subnet mask
- IPv6 address and prefix
- VLAN assignment
- Status (up, down, disabled)

IPv6 Interface Information

The following command displays IPv6 interface information:

```
show ipv6 interface <interface number>
```

Command mode: All

```
Interface information:
  2: IP6 2001:0:0:0:225:3ff:febb:bb15/64             , vlan 1, up
         fe80::225:3ff:febb:bb15
    Link local address:
        fe80::225:3ff:febb:bb15
    Global unicast address(es):
        2001::225:3ff:febb:bb15/64
    Anycast address(es):
        Not Configured.
    Joined group address(es):
        ff02::1
        ff02::2
        ff02::1:ffbb:bb15
    MTU is 1500
    ICMP redirects are enabled
    ND DAD is enabled, Number of DAD attempts: 1
    ND router advertisement is disabled
```

For each interface, the following information is displayed:

- IPv6 interface address and prefix
- VLAN assignment
- Status (up, down, disabled)
- Path MTU size
- Status of ICMP redirects
- Status of Neighbor Discovery (ND) Duplicate Address Detection (DAD)
- Status of Neighbor Discovery router advertisements

IPv6 Path MTU Information

The following command displays IPv6 Path MTU information:

`show ipv6 pmtu [<`*destination IPv6 address*`>]`

Command mode: All

```
Path MTU Discovery info:
Max Cache Entry Number : 10
Current Cache Entry Number: 2
Cache  Timeout Interval : 10 minutes
Destination Address                     Since       PMTU
5000:1::3                               00:02:26    1400
FE80::203:A0FF:FED6:141D                00:06:55    1280
```

Path MTU Discovery information provides information about entries in the Path MTU cache. The PMTU field indicates the maximum packet size in octets that can successfully traverse the path from the switch to the destination node. It is equal to the minimum link MTU of all the links in the path to the destination node.

IP Information

The following command displays Layer 3 information:

`show ip interface brief`

Command mode: All

IP information includes:

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

Quality of Service Information

Table 29. QoS Information Options

Command Syntax and Usage
`show qos random-detect` Displays WRED ECN information. **Command mode:** All

Access Control List Information Commands

Table 30. ACL Information Options

Command Syntax and Usage
`show access-control list` <*ACL number*> Displays ACL list information. For details, see page 46. **Command mode:** All
`show access-control list6` <*ACL number*> Displays IPv6 ACL list information. **Command mode:** All
`show access-control group` <*ACL group number*> Displays ACL group information. **Command mode:** All

Access Control List Information

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

`show access-control list <ACL number>`

Command mode: All

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

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

Table 31. ACL Parameter Descriptions

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

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 RMON Lrn Fld PVID     DESCRIPTION              VLAN(s)
             Trk               NVLAN
------- ---- --- ---- --- --- ------ -------------- --------------------------------
EXT3    45    n   d    e   e  4081#  EXT3           4081
EXT4    46    n   d    e   e  4081#  EXT4           4081
EXT5    47    n   d    e   e  4081#  EXT5           4081
EXT6    48    n   d    e   e  4081#  EXT6           4081
EXT7    49    n   d    e   e  4081#  EXT7           4081
EXT8    50    n   d    e   e  4081#  EXT8           4081
EXT9    51    n   d    e   e  4081#  EXT9           4081
EXT10   52    n   d    e   e  4081#  EXT10          4081
EXT11   53    n   d    e   e  4083#  EXT11          4083
EXT12   54    n   d    e   e  4083#  EXT12          4083
EXT13   55    n   d    e   e  4083#  EXT13          4083
EXT14   56    n   d    e   e  4083#  EXT14          4083
EXT15   57    n   d    e   e  4082#  EXT15          4082
EXT16   58    n   d    e   e  4082#  EXT16          4082
EXT17   59    n   d    e   e  4082#  EXT17          4082
EXT18   60    n   d    e   e  4082#  EXT18          4082
EXT19   61    n   d    e   e  4082#  EXT19          4082
EXT20   62    n   d    e   e  4082#  EXT20          4082
EXT21   63    n   d    e   e  4082#  EXT21          4082
EXT22   64    n   d    e   e  4082#  EXT22          4082
EXTM    65    n   d    e   e  4095   EXTM           4095
MGT1    66    y   d    e   e  4095   MGT1           4095

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

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of 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 uses PVID/Native-VLAN tagging or not (`y` or `n`)
- Whether the port uses PVID ingress tagging or not (`y` or `n`)
- Whether the port is internal, external or used for management
- Whether the port has FDB Learning enabled (`Lrn`)
- Whether the port has Port Flooding enabled (`Fld`)
- Port VLAN ID (PVID/Native-VLAN)
- Port description
- VLAN membership

Port Transceiver Status

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

```
show interface transceiver
```

Command mode: All

```
Port             Link  Transceiver    Vendor           Part             Approve
---------------- ----- -------------- ---------------- ---------------- --------
49 EXT21         Down  SX SFP         Blade Network    BN-CKM-S-SX      Approved
50 EXT22         LINK  3m DAC         BLADE NETWORK    BN-SP-CBL-3M     Accepted
51 EXT23         LINK  SR SFP+        Blade Network    BN-CKM-SP-SR     Approved
52 EXT24         LINK  SR SFP+        Blade Network    BN-CKM-SP-SR     Approved
```

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

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

Use the following command to display extended transceiver information:

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

Command mode: All

```
Port             TX  Link  TXFlt Volts DegsC TXuW  RXuW  Transceiver    Approve
---------------- --- ----- ----- ----- ----- ----- ----- -------------- --------
49 EXT21         Ena Down  NoFlt  3.24 40.0  287.2   0.0 SX SFP         Approved
         Blade Network    Part:BN-CKM-S-SX      Date:110225 S/N:BNTM1108QB
```

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

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

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

Table 32. Expected Transceiver Optical Power Levels

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

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

Virtual Machines Information

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

Table 33. Virtual Machines Information Options

Command Syntax and Usage
`show virt port` <*port alias or number*> Displays Virtual Machine information for the selected port. **Command mode:** All
`show virt vm [-v]` Displays all Virtual Machine information. – `-v` displays verbose information **Command mode:** All

VM Information

The following command displays VM information:

`show virt vm`

Command mode: All

```
IP Address       VMAC Address        Index Port    VM Group (Profile)
---------------- -----------------   ----- ------- ------------------
*127.31.46.50    00:50:56:4e:62:f5   4     INT3
*127.31.46.10    00:50:56:4f:f2:85   2     INT4
+127.31.46.51    00:50:56:72:ec:86   1     INT3
+127.31.46.11    00:50:56:7c:1c:ca   3     INT4
 127.31.46.25    00:50:56:9c:00:c8   5     INT4
 127.31.46.15    00:50:56:9c:21:2f   0     INT4
 127.31.46.35    00:50:56:9c:29:29   6     INT3

Number of entries: 8
* indicates VMware ESX Service Console Interface
+ indicates VMware ESX/ESXi VMKernel or Management Interface
```

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

- IP address
- MAC address
- Index number assigned to the VM
- Internal port on which the VM was detected
- VM group that contains the VM, if applicable

VM Check Information

The following command displays VM Check information:

```
show virt vmcheck
```

Command mode: All

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

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

VMware Information

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

Table 34. VMware Information Options

Command Syntax and Usage
`show virt vmware hosts` Displays a list of VMware hosts. **Command mode:** All
`show virt vmware hello` Displays VMware hello settings. **Command mode:** All
`show virt vmware showhost` *<host UUID>* | *<host IP address>* | *<host name>* Displays detailed information about a specific VMware host. **Command mode:** All
`show virt vmware showvm` *<VM UUID>* | *<VM IP address>* | *<VM name>* Displays detailed information about a specific Virtual Machine (VM). **Command mode:** All
`show virt vmware vms` Displays a list of VMs. **Command mode:** All

VMware Host Information

The following command displays VM host information:

```
show virt vmware hosts
```

Command mode: All

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

VM host information includes the following:

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

EVB Information

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

Table 35. EVB Information Options

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

UFP Information

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

Table 36. UFP Information Options

Command Syntax and Usage
`show ufp [port <port_no.>] [vport <1-4>] [network|qos|evb]` Displays the UFP network and QoS settings applied on all ports or on specified physical and virtual ports. – `network` filters only UFP network settings – `qos` filters only QoS network settings – `evb` filters only EVB profile settings **Command mode:** All
`show ufp information port [<port_no.>]` Displays UFP status for all physical ports or only for a specified physical port. Information includes wether the UFP is enabled on the physical port, how many virtual ports are enabled and the link stats for each virtual port. For details, see page 55. **Command mode:** All
`show ufp information {cdcp|qos|tlvstat} [port <port_no.>]` Displays global or port-specific UFP information on: – `cdcp` displays S-Channel Discovery and Configuration Protocol (CDCP) information. CDCP allows hypervisor hosts to create on-demand S-channels with the switch. For details, see page 55. – `qos` displays bandwidth allocation between virtual ports. For details, see page 56. – `tlvstat` displays status for Type-Length-Values transmitted on UFP-enabled physical ports. For details, see page 56. **Command mode:** All
`show ufp information qos [port <port_no.>] [vport <1-4>]` Displays bandwidth allocation between virtual ports for all physical ports or specified physical and virtual ports. **Command mode:** All
`show ufp information vport [port <port_no.>] [vport <1-4>]` Displays state, operating mode and VLAN related information for all virtual ports, for virtual ports belonging to a specified physical port or for a single virtual port. For details, see page 57. **Command mode:** All
`show ufp information getvlan <2-4094>` Displays state, operating mode and VLAN related information for physical and virtual ports associated to a specified VLAN ID. **Command mode:** All

Table 36. UFP Information Options

Command Syntax and Usage
`show ufp information vlan [<1-4094>]` Displays ports and vports associated to all configured VLANs or to a specified VLAN ID. For details, see page 58. **Command mode:** All
`show ufp {receive|transmit} {cap|cdcp} port <port_no.>` Displays received/transmitted Type-Length-Values for the specified ports. – `cap` displays the UFP Capability Discovery TLV – `cdcp` displays the UFP Channel Discovery and Configuration Protocol TLV For details, see page 58. **Command mode:** All

Port Information

The following command displays UFP port information:

```
show ufp information port
```

Command mode: All

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

Port information includes the following for each physical port:

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

CDCP Information

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

```
show ufp information cdcp
```

Command mode: All

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

CDCP information includes the following for each physical port:

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

QoS Information

The following command displays Quality of Service information:

```
show ufp information qos
```

Command mode: All

```
Global UFP QOS mode: UFP QOS BW

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

QoS information includes the following:

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

TLV Status Information

The following command displays Type-Length-Values information:

```
show ufp information tlvstat
```

Command mode: All

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

TLV status information includes the following:

- Physical port alias
- Type-Length-Values status

Virtual Port Information

The following command displays virtual port information:

```
show ufp information vport
```

Command mode: All

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

Virtual port information includes the following for each virtual port:

- Virtual port number
- Channel status
- Operating mode (trunk, access, tunnel, auto or FCoE)
- S-channel VLAN ID

- Default VLAN ID
- Default VLAN ID tagging enforcement
- EVB profile
- VLANs the virtual port is associated with

VLAN Information

The following command displays VLAN information:

```
show ufp information vlan
```

Command mode: All

```
----
VLAN
----
 100

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

EXT Port list:
   EXT3     EXT4     EXT8     EXT9

INT Port list:
 INTB13

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

VMR Port list:
```

VLAN information includes the following for each VLAN:

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

TLV Information

The following commands display TLV information:

```
show ufp receive cap port <port_no.>
```

Command mode: All

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

UFP Capability Discovery TLV information includes the following:

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

`show ufp transmit cdcp port <`*port_no.*`>`

Command mode: All

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

UFP Channel Discovery and Configuration Protocol TLV includes the following:

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

Converged Enhanced Ethernet Information

Table 37 describes the Converged Enhanced Ethernet (CEE) information options.

Table 37. CEE Information Options

Command Syntax and Usage
`show cee information` Displays all CEE information **Command mode:** All

DCBX Information

Table 38 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 38. DCBX Information Options

Command Syntax and Usage
`show cee information dcbx port <`*port alias or number*`> control` Displays information about the DCBX Control state machine for the selected port. For details, see page 61. **Command mode:** All
`show cee information dcbx port <`*port alias or number*`> feature` Displays information about the DCBX Feature state machine for the selected port. For details, see page 62. **Command mode:** All
`show cee information dcbx port <`*port alias or number*`> ets` Displays information about the DCBX ETS state machine. For details, see page 62. **Command mode:** All
`show cee information dcbx port <`*port alias or number*`> pfc` Displays information about the DCBX PFC state machine. For details, see page 64. **Command mode:** All
`show cee information dcbx port <`*port alias or number*`> app_proto` Displays information about the DCBX Application Protocol state machine on the selected port. For details, see page 65. **Command mode:** All
`show cee information dcbx port <`*port alias or number*`>` Displays all DCBX information. **Command mode:** All

DCBX Control Information

The following command displays DCBX control information:

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

Command mode: All

```
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 39. DCBX Feature Information Fields

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

DCBX ETS Information

The following command displays DCBX ETS information:

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

Command mode: All

```
DCBX Port Priority Group - Priority Allocation Table
====================================================
Alias  Port Priority PgIdDes PgIdOper PgIdPeer
------ ---- -------- ------- -------- --------
INTA2  2    0        PGID0   PGID0    PGID0
INTA2  2    1        PGID0   PGID0    PGID0
INTA2  2    2        PGID0   PGID0    PGID0
INTA2  2    3        PGID1   PGID1    PGID1
INTA2  2    4        PGID2   PGID2    PGID0
INTA2  2    5        PGID2   PGID2    PGID0
INTA2  2    6        PGID2   PGID2    PGID0
INTA2  2    7        PGID2   PGID2    PGID0

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

The following table describes the DCBX ETS information.

Table 40. 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 41. DCBX Application Protocol Information Fields

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

Table 41. 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 42 describes the Enhanced Transmission Selection (ETS) information options

Table 42. ETS Information Options

Command Syntax and Usage
`show cee global ets information` Displays global ETS information. **Command mode:** All

The following command displays ETS information:

```
show cee global ets information
```

Command mode: All

```
Global ETS information:

Number of COSq: 8

Mapping of 802.1p Priority to Priority Groups:

Priority  PGID  COSq
--------  ----  ----
    0       0     0
    1       0     0
    2       0     0
    3       1     1
    4       2     2
    5       2     2
    6       2     2
    7       2     2

Bandwidth Allocation to Priority Groups:

PGID  PG%  Description
----  ---  -----------
  0    10
  1    50
  2    40
```

Enhanced Transmission Selection (ETS) information includes the following:

- Number of Class of Service queues (COSq) configured
- 802.1p mapping to Priority Groups and Class of Service queues
- Bandwidth allocated to each Priority Group

PFC Information

Table 43 describes the Priority Flow Control (PFC) information options.

Table 43. PFC Information Options

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

The following command displays PFC information for a port:

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

Command mode: All

```
Global PFC Information:

PFC - ON

Priority   State   Description
--------   -----   -----------
   0        Dis
   1        Dis
   2        Dis
   3        Ena
   4        Dis
   5        Dis
   6        Dis
   7        Dis
------------------------------------------------------------------------
State - indicates whether PFC is Enabled/Disabled on a particular priority
```

FCoE Information

Table 44 describes the Fibre Channel over Ethernet (FCoE) information options.

Table 44. FCoE Information Options

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

FIP Snooping Information

Table 45 describes the Fibre Channel Initialization Protocol (FIP) Snooping information options

Table 45. FIP Snooping Information Options

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

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

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

Command mode: All

```
FIP Snooping on port INTA2:
This port has been configured to automatically detect FCF.
It has currently detected to have 0 FCF connecting to it.
FIPS ACLs configured on this port:
SMAC 00:c0:dd:13:9b:6f, action deny.
SMAC 00:c0:dd:13:9b:70, action deny.
SMAC 00:c0:dd:13:9b:6d, action deny.
SMAC 00:c0:dd:13:9b:6e, action deny.
DMAC 00:c0:dd:13:9b:6f, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:70, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6d, ethertype 0x8914, action permit.
DMAC 00:c0:dd:13:9b:6e, ethertype 0x8914, action permit.
SMAC 0e:fc:00:01:0a:00, DMAC 00:c0:dd:13:9b:6d, ethertype 0x8906, vlan 1002, action
permit.
DMAC 01:10:18:01:00:01, Ethertype 0x8914, action permit.
DMAC 01:10:18:01:00:02, Ethertype 0x8914, action permit.
Ethertype 0x8914, action deny.
Ethertype 0x8906, action deny.
SMAC 0e:fc:00:00:00:00, SMAC mask ff:ff:ff:00:00:00, action deny.
```

FIP Snooping port information includes the following:

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

Information Dump

The following command dumps switch information:

```
show information-dump
```

Command mode: All

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

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

Chapter 3. Statistics Commands

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

Table 46. Statistics Commands

Command Syntax and Usage
`show layer3 counters` **Command mode:** All Displays Layer 3 statistics.
`show snmp-server counters` **Command mode:** All Displays SNMP statistics. See page 116 for sample output.
`show ntp counters` Displays Network Time Protocol (NTP) Statistics. **Command mode:** All See page 120 for a sample output and a description of NTP Statistics.
`show counters` Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. **Command mode:** All For details, see page 122.

Port Statistics

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

Table 47. Port Statistics Commands

Command Syntax and Usage
`show interface port <port alias or number> bridging-counters` Displays bridging (“dot1”) statistics for the port. See page 75 for sample output. **Command mode:** All
`show interface port <port alias or number> ethernet-counters` Displays Ethernet (“dot3”) statistics for the port. See page 76 for sample output. **Command mode:** All
`show interface port <port alias or number> interface-counters` Displays interface statistics for the port. See page 79 for sample output. **Command mode:** All
`show interface port <port alias or number> ip-counters` Displays IP statistics for the port. See page 81 for sample output. **Command mode:** All
`show interface port <port alias or number> link-counters` Displays link statistics for the port. See page 81 for sample output. **Command mode:** All
`show interface port <port alias or number> oam counters` Displays Operation, Administrative, and Maintenance (OAM) protocol statistics for the port. **Command mode:** All
`clear interface port <port alias or number> counters` Clears all statistics for the port. **Command mode:** All except User EXEC
`clear counters` Clears statistics for all ports. **Command mode:** All except User EXEC

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 48. 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 49. Ethernet Statistics for Port

Statistics	Description
dot3StatsAlignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `frameCheckError` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 49. Ethernet Statistics for Port (continued)

Statistics	Description
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
dot3StatsMultipleCollisionF rames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMac TransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3StatsCarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 49. Ethernet Statistics for Port (continued)

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

Interface Statistics

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

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

Command mode: All

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


Ingress Discard reasons:                 Egress Discard reasons:

VLAN Discards:                     0     HOL-blocking Discards:             0
Filter Discards:                   0     MMU Discards:                      0
Policy Discards:                   0     Cell Error Discards:               0
Non-Forwarding State:              0     MMU Aging Discards:                0
IBP/CBP Discards:                  0     Other Discards:                   11
```

Table 50. 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 50. Interface Statistics for Port (continued)

Statistics	Description
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`.
ifOutMulticastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.
ifOutFlowControlPkts	The total number of flow control `pause` packets transmitted out of the interface.
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

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 51. 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 52. Link Statistics

Statistics	Description
linkStateChange	The total number of link state changes.

Trunk Group Statistics

Table 53. Trunk Group Statistics Commands

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

Layer 2 Statistics

Table 54. Layer 2 Statistics Commands

Command Syntax and Usage
`show interface port <port alias or number> lacp counters` Displays Link Aggregation Control Protocol (LACP) statistics. See page 84 for sample output. **Command mode:** All
`clear interface port <port alias or number> lacp counters` Clears Link Aggregation Control Protocol (LACP) statistics. **Command mode:** All except User EXEC
`show interface port <port alias or number> lldp counters` Displays LLDP statistics. See page 85 for sample output. **Command mode:** All except User EXEC
`show oam counters` Displays OAM statistics. See page 86 for sample output. **Command mode:** All except User EXEC

LACP Statistics

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

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

Command mode: All

```
Port EXT1:
 -------------------------------------
 Valid LACPDUs received:         - 870
 Valid Marker PDUs received:     - 0
 Valid Marker Rsp PDUs received: - 0
 Unknown version/TLV type:       - 0
 Illegal subtype received:       - 0
 LACPDUs transmitted:            - 6031
 Marker PDUs transmitted:        - 0
 Marker Rsp PDUs transmitted:    - 0
```

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

Table 55. 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 56. LLDP Port Statistics

Statistic	Description
`Frames Transmitted`	Total number of LLDP frames transmitted.
`Frames Received`	Total number of LLDP frames received.
`Frames Received in Errors`	Total number of LLDP frames that had errors.
`Frames Discarded`	Total number of LLDP frames discarded.
`TLVs Unrecognized`	Total number of unrecognized TLV (Type, Length, and Value) fields received.
`Neighbors Aged Out`	Total number of neighbor devices that have had their LLDP information aged out.

OAM Statistics

Use the following command to display OAM statistics:

```
show oam counters
```

Command mode: All

```
OAM statistics on port INT1
---------------------------------------
Information OAMPDU Tx :      0
Information OAMPDU Rx :      0
Unsupported OAMPDU Tx :      0
Unsupported OAMPDU Tx :      0

Local faults
-------------
    0 Link fault records
    0 Critical events
    0 Dying gasps

Remote faults
-------------
    0 Link fault records
    0 Critical events
    0 Dying gasps
```

OAM statistics include the following:

- Total number of OAM Protocol Data Units (OAMPDU) transmitted and received.
- Total number of unsupported OAM Protocol Data Units (OAMPDU) transmitted and received.
- Local faults detected
- Remote faults detected

Layer 3 Statistics

Table 57. Layer 3 Statistics Commands

Command Syntax and Usage
`show ip counters` Displays IP statistics. See page 88 for sample output. **Command mode:** All
`clear ip counters` Clears IPv4 statistics. Use this command with caution as it deletes all the IPv4 statistics. **Command mode:** All except User EXEC
`show ip dns counters` Displays Domain Name System (DNS) statistics. See page 90 for sample output. **Command mode:** All
`show ip tcp counters` Displays TCP statistics. See page 91 for sample output. **Command mode:** All
`show ip udp counters` Displays UDP statistics. See page 92 for sample output. **Command mode:** All
`show ip igmp counters` Displays IGMP statistics. See page 94 for sample output. **Command mode:** All
`show ip igmp vlan <`*vlan number*`> counters` Displays IGMP statistics for a specific VLAN. See page 94 for sample output. **Command mode:** All
`clear ip dns counters` Clears Domain Name System (DNS) statistics. **Command mode:** All except User EXEC
`clear ip tcp counters` Clears Transmission Control Protocol (TCP) statistics. **Command mode:** All except User EXEC
`clear ip udp counters` Clears User Datagram Protocol (UDP) statistics. **Command mode:** All except User EXEC

Table 57. Layer 3 Statistics Commands (continued)

Command Syntax and Usage
`clear ip igmp [<VLAN number>] counters` Clears IGMP statistics for all VLANs or for a specific VLAN. **Command mode:** All
`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 58. 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 58. IP Statistics (continued)

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

Table 58. IP Statistics (continued)

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

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 59. 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 60. TCP Statistics

Statistic	Description
tcpRtoAlgorithm	The algorithm used to determine the `timeout` value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Table 60. 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 61. UDP Statistics

Statistic	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

IGMP Statistics

The following command displays statistics about IGMP protocol packets for all VLANs:

```
show ip igmp counters
```

Command mode: All

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

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

```
show ip igmp vlan <vlan number> counters
```

Command mode: All

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

Table 62. IGMP Statistics

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received for specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpDiscardPkts	Total number of IGMP packets discarded
rxIgmpLeaves	Total number of Leave requests received

Table 62. IGMP Statistics

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

Management Processor Statistics

Table 63. Management Processor Statistics Commands

Command Syntax and Usage
`show mp thread` Displays STEM thread statistics. This command is used by Technical Support personnel. **Command mode:** All
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see page 97. **Command mode:** All
`show mp tcp-block` Displays all TCP control blocks that are in use. To view a sample output and a description of the statistics, see page 108. **Command mode:** All
`show mp udp-block` Displays all UDP control blocks that are in use. To view a sample output, see page 109. **Command mode:** All
`show processes cpu` Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 109. **Command mode:** All
`show processes cpu history` Displays history of CPU utilization. To view a sample output, see page 112. **Command mode:** All

Packet Statistics

Table 64. Packet Statistics Commands

Command Syntax and Usage
`show mp packet counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 97. **Command mode:** All
`clear mp packet logs` Clears all CPU packet statistics and logs. **Command mode:** All

MP Packet Statistics

The following command displays MP packet statistics:

```
show mp packet counters
```

Command mode: All 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 65. 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: – IGMP – PIM – ICMP requests – ICMP replies
TCP packets	Total number of TCP packets received and sent. Includes the following packet types: – FTP – HTTP – SSH – TACACS+ – Telnet – Other
UDP packets	Total number of UDP packets received and sent. Includes the following packet types: – DHCP – NTP – RADIUS – SNMP – TFTP – Other
RIP packets	Total number of Routing Information Protocol packets received and sent.

Table 65. 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 65. 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 66. Packet Statistics Log Options

Command Syntax and Usage
`show mp packet log all` Displays all packet logs received by and sent from the CPU. To view a sample output and a description of the log entries, see "Packet Log example" on page 103.
`show mp packet log rx` Displays all packets logs received by the CPU.
`show mp packet log tx` Displays all packet logs sent from the CPU.

Packet Log example

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

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

Each packet log entry includes the following information:

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

Packet Statistics Last Packet

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

Table 67. Last Packet Options

Command Syntax and Usage
`show mp packet last both` *<1-1000>* Displays a specified number of recent packet logs received by and sent from the CPU. To view a sample output and a description, see "Packet Log example" on page 103.
`show mp packet last rx` *<1-1000>* Displays a specified number of recent packet logs received by the CPU.
`show mp packet last tx` *<1-1000>* Displays a specified number of recent packet logs sent from the CPU.

Packet Statistics Dump

The following table describes the Packet Statistics Dump options.

Table 68. Packet Statistics Dump Options

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

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 69.

Table 69. Packet Log Parsing Options

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

Table 69. Packet Log Parsing Options (continued)

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

Table 69. Packet Log Parsing Options (continued)

Command Syntax and Usage
`show mp packet parse rx|tx port` <*port_number*> Displays only logged packets with the specified port. **Command mode:** All
`show mp packet parse rx|tx mac` <*MAC_address*> Displays only logged packets with the specified MAC address. **Command mode:** All
`show mp packet parse rx|tx ip-addr` <*IPv4_address*> Displays only logged packets with the specified IPv4 address. **Command mode:** All
`show mp packet parse rx|tx other` Displays logs of all packets not explicitly selectable. **Command mode:** All
`show mp packet parse rx|tx raw` Displays raw packet buffer in addition to headers. **Command mode:** All

TCP Statistics

The following command displays TCP statistics:

```
show mp tcp-block
```

Command mode: All

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


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

Table 70. 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 71. 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 71. 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 72. 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 73. ACL Statistics Commands

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

ACL Statistics

The following command displays ACL statistics.

```
show access-control counters
```

Command mode: All

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

Fibre Channel over Ethernet Statistics

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

```
show fcoe counters
```

Command mode: All

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

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

Table 74. FCoE Statistics

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

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

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

```
clear fcoe counters
```

Command mode: All

SNMP Statistics

The following command displays SNMP statistics:

```
show snmp-server counters
```

Command mode: All except User EXEC

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

Table 75. 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 75. SNMP Statistics (continued)

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

Table 75. SNMP Statistics (continued)

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

Table 75. SNMP Statistics (continued)

Statistic	Description
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpSilentDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMPv2 entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	The total number of `GetRequest`-PDUs, `GetNextRequest`-PDUs, `GetBulkRequest`-PDUs, `SetRequest`-PDUs, and `InformRequest`-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the message to a proxy target failed in a manner such that no Response-PDU could be returned.

NTP Statistics

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

The following command displays NTP statistics:

```
show ntp counters
```

Command mode: All

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

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

Table 76. NTP Statistics

Field	Description
Primary Server	• **Requests Sent:** The total number of NTP requests the switch sent to the primary NTP server to synchronize time. • **Responses Received:** The total number of NTP responses received from the primary NTP server. • **Updates:** The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	• **Requests Sent:** The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. • **Responses Received:** The total number of NTP responses received from the secondary NTP server. • **Updates:** The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.

Table 76. NTP Statistics (continued)

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

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 77. General Configuration Commands

Command Syntax and Usage
`show running-config` Dumps current configuration to a script file. **Command mode:** Privileged EXEC For details, see page 250.
`show running-config diff` Displays running configuration changes that have been applied but not saved to flash memory. **Command mode:** Privileged EXEC
`copy running-config backup-config` Copy the current (running) configuration from switch memory to the `backup-config` partition. **Command mode:** Privileged EXEC For details, see page 251.
`copy running-config startup-config` Copy the current (running) configuration from switch memory to the `startup-config` partition. **Command mode:** Privileged EXEC
`copy running-config {ftp|tftp|sftp} [extm-port|mgt-port]` Backs up current configuration to a file on the selected FTP/TFTP/SFTP server. Select a management port, or press **Enter** to use the default (management) port. **Command mode:** Privileged EXEC
`copy {ftp|tftp|sftp} running-config [extm-port|mgt-port]` Restores current configuration from a FTP/TFTP/SFTP server. Select a management port, or press **Enter** to use the default (management) port. **Command mode:** Privileged EXEC For details, see page 252.

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 268.

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 78. System Configuration Commands

Command Syntax and Usage
`system date <yyyy> <mm> <dd>` Prompts the user for the system date. The date retains its value when the switch is reset. **Command mode:** Global configuration
`system time <hh>:<mm>:<ss>` Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset. **Command mode:** Global configuration
`system timezone` Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Saving Time, etc. **Command mode:** Global configuration
`[no] system daylight` Disables or enables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled. **Command mode:** Global configuration
`terminal-length <0-300>` Configures the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding `line vty length` or `line console length` value in effect at login. **Command mode:** All
`line console length <0-300>` Configures the number of lines per screen displayed in the CLI by default for console sessions. Setting it to 0 disables paging. The default value is 28. **Command mode:** Global configuration
`no line console` Sets `line console length` to the default value of 28. **Command mode:** Global configuration
`line vty length <0-300>` Sets the default number of lines per screen displayed for Telnet and SSH sessions. A value of 0 disables paging. The default value is 28. **Command mode:** Global configuration

Table 78. System Configuration Commands (continued)

Command Syntax and Usage
`no line vty` Sets `line vty length` to the default value of 28. **Command mode:** Global configuration
`system idle` <*0-60*> Sets the idle timeout for CLI sessions in minutes. The default value is 10 minutes. A value of 0 disables system idle. **Command mode:** Global configuration
`system linkscan {fast|normal|slow}` Configures the link scan interval used to poll the status of ports. **Command mode:** Global configuration
`system notice` <*maximum 1024 character multi-line login notice*> <`'.'` *to end*> Displays a login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines. **Command mode:** Global configuration
[no] `banner` <*1-80 characters*> Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `show sys-info` command. **Command mode:** Global configuration
[no] `hostname` <*character string*> Enables or disables displaying of the host name (system administrator’s name) in the Command Line Interface (CLI). **Command mode:** Global configuration
[no] `system dhcp [extm|mgt]` Enables or disables Dynamic Host Control Protocol for setting the IP address on the selected interface. When enabled, the IP address obtained from the DHCP server overrides the static IP address. The default setting is `enabled`. **Command mode:** Global configuration
[no] `system reset-control` Enables or disables the reset control flag. When enabled, the switch continues to function after a crash of the main processor, using the last known Layer 2/3 information. **Command mode:** Global configuration
[no] `system packet-logging` Enables or disables logging of packets that come to the CPU. The default setting is `enabled`. **Command mode:** Global configuration

Table 78. System Configuration Commands (continued)

Command Syntax and Usage
`[no] boot strict enable` Enables or disables switch operation in security strict mode. When enabled, the authentication and privacy protocols and algorithms of the device are compliant with NIST SP-800-131A, with non-compliant protocols and algorithms disabled. Setting will be applied and device will be reset to default factory configuration after reboot. The default setting is `disabled`. **Command mode:** Global configuration
`show boot strict` Displays the current security strict mode status. **Command mode:** Global configuration
`show system` Displays the current system parameters. **Command mode:** All

System Error Disable and Recovery Configuration

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

Table 79. Error Disable Configuration Commands

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

System Host Log Configuration

Table 80. 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
[no] logging synchronous [level <*0-7*> | all] Enables or disables synchronous logging messages. When enabled, logging messages are displayed asynchronously. The level parameter sets the message severity level. Messages with a severity level equal to or higher than this value are displayed asynchronously. Low numbers indicate greater severity. All displays all messages asynchronously, regardless the severity level. The default setting is 2. **Command mode:** Global configuration

Table 80. Host Log Configuration Commands

Command Syntax and Usage
`logging console severity <0-7>` Sets the severity level of system log messages to display via the console, Telnet, and SSH. The system displays only messages with the selected severity level and above. For example, if you set the console severity to 2, only messages with severity level of 1 and 2 are displayed. The default is 7, which means log all severity levels. **Command mode:** Global configuration
`no logging console severity` Disables delivering syslog messages to the console based on severity. **Command mode:** Global configuration
[no] `logging buffer severity <0-7>` Sets the severity level of system log messages that are written to flash buffer. The system saves only messages with the selected severity level and above. For example, if you set the buffer severity to 2, only messages with severity level of 1 and 2 are saved. **Command mode**: Global configuration
[no] `logging log` [<*feature*>] Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as `vlans`, `stg`, or `ssh`), or enable/disable syslog on all available features. **Command mode:** Global configuration
`[no] logging pdrop enable` Enables or disables packet drop logging. By default, the switch generates these messages once every 30 minutes. **Command mode:** Global configuration
`logging pdrop interval <0-30>` Sets the packet drop logging interval. The default value is `30`. **Command mode:** Global configuration
`show logging [severity <`*severity level*`>] [reverse]` Displays the current syslog settings, followed by the most recent 2000 syslog messages, as displayed by the `show logging messages` command. For details, see page 23. The `reverse` option displays the output in reverse order, from the newest entry to the oldest. **Command mode:** All

SSH Server Configuration

For the SI4093 10Gb System Interconnect Module (SIM), these commands enable Secure Shell access from any SSH client.

Table 81. SSH Server Configuration Commands

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

RADIUS Server Configuration

Table 82. 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

Table 82. RADIUS Server Configuration Commands

Command Syntax and Usage
`[no] radius-server secure-backdoor` Enables or disables the RADIUS backdoor using secure password for Telnet/SSH/HTTP/HTTPS. This command does not apply when RADIUS backdoor is enabled. **Command mode:** Global configuration
`radius-server enable` Enables the RADIUS server. **Command mode:** Global configuration
`no radius-server enable` Disables the RADIUS server. **Command mode:** Global configuration
`show radius-server` Displays the current RADIUS server parameters. **Command mode:** All

TACACS+ Server Configuration

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

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

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

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

Table 83. TACACS+ Server Configuration Commands

Command Syntax and Usage
[no] `tacacs primary-host` <*IP address*> Defines the primary TACACS+ server address. **Command mode:** Global configuration
[no] `tacacs secondary-host` <*IP address*> Defines the secondary TACACS+ server address. **Command mode:** Global configuration
[no] `tacacs primary-host` <*IP address*> `key` <*1-32 characters*> This is the primary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[no] `tacacs secondary-host` <*IP address*> `key` <*1-32 characters*> This is the secondary shared secret between the switch and the TACACS+ server(s). **Command mode:** Global configuration
[`default`] `tacacs port` <*TCP port number*> Enter the number of the TCP port to be configured, between 1 and 65000. The default is 49. **Command mode:** Global configuration
`tacacs retransmit` <*1-3*> Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests. **Command mode:** Global configuration

Table 83. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
`tacacs attempts <1-10>` Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts. **Command mode:** Global configuration
`tacacs timeout <4-15>` Sets the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default is 5 seconds. **Command mode:** Global configuration
`[no] tacacs user-mapping {<0-15> user|oper|admin}` Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level. **Command mode:** Global configuration
`[no] tacacs backdoor` Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS. Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding. The default setting is `disabled`. To obtain the TACACS+ backdoor password for your SI4093, contact your Service and Support line. **Command mode:** Global configuration
`[no] tacacs secure-backdoor` Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding. This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port. The default is `disabled`. **Command mode:** Global configuration
`[no] tacacs privilege-mapping` Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`. **Command mode:** Global configuration

Table 83. TACACS+ Server Configuration Commands (continued)

Command Syntax and Usage
`[no] tacacs-server password-change` Enables or disables TACACS+ password change. The default value is `disabled`. **Command mode:** Global configuration
`primary-password` Configures the password for the primary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
`secondary-password` Configures the password for the secondary TACACS+ server. The CLI will prompt you for input. **Command mode:** Global configuration
`[no] tacacs-server command-authorization` Enables or disables TACACS+ command authorization. **Command mode:** Global configuration
`[no] tacacs-server command-logging` Enables or disables TACACS+ command logging. **Command mode:** Global configuration
`[no] tacacs-server directed-request [restricted|no-truncate]` Enables or disables TACACS+ directed request, which uses a specified TACACS+ server for authentication, authorization, accounting. When enabled, When directed-request is enabled, each user must add a configured TACACS+ server hostname to the username (for example, `username@hostname`) during login. This command allows the following options: – **Restricted**: Only the username is sent to the specified TACACS+ server. – **No-truncate**: The entire login string is sent to the TACACS+ server. **Command mode:** Global configuration
`[no] tacacs-server enable` Enables or disables the TACACS+ server. By default, the server is disabled. **Command mode:** Global configuration
`[no] tacacs-server accounting-enable` Enables or disables TACACS+ accounting. **Command mode:** Global configuration
`show tacacs-server` Displays current TACACS+ configuration parameters. **Command mode:** All

LDAP Server Configuration

LDAP (Lightweight Directory Access Protocol) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

Table 84. LDAP Server Configuration Commands

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

Table 84. LDAP Server Configuration Commands (continued)

Command Syntax and Usage
`ldap-server enable` Enables the LDAP server. **Command mode:** Global configuration
`no ldap-server enable` Disables the LDAP server. **Command mode:** Global configuration
`show ldap-server` Displays the current LDAP server parameters. **Command mode:** All

NTP 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 85. NTP Server Configuration Commands

Command Syntax and Usage
[no] ntp primary-server <*IP address*>[extm-port|mgt-port] Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: – internal management port (mgt) – external management port (extm) **Command mode:** Global configuration
[no] ntp secondary-server <*IP address*>[extm-port|mgt-port] Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: – internal management port (mgt) – external management port (extm) **Command mode:** Global configuration
[no] ntp ipv6 primary-server <*IPv6 address*>[extm-port|mgt-port] Prompts for the IPv6 addresses of the primary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: – internal management port (mgt) – external management port (extm) **Note**: To delete the IPv6 primary server, use the following command: no ntp ipv6 primary-server <*IPv6 address*> **Command mode:** Global configuration
[no] ntp ipv6 secondary-server <*IPv6 address*>[extm-port|mgt-port] Prompts for the IPv6 addresses of the secondary NTP server to which you want to synchronize the switch clock. Select the port to use for data transfer: – internal management port (mgt) – external management port (extm) **Note**: To delete the IPv6 secondary server, use the following command: no ntp ipv6 secondary-server <*IPv6 address*> **Command mode:** Global configuration
ntp interval <*5-44640*> Specifies the interval, that is, how often, in minutes, to re-synchronize the switch clock with the NTP server. The default value is 1440. **Command mode:** Global configuration

Table 85. NTP Server Configuration Commands

Command Syntax and Usage
`[no] ntp authenticate` Enables or disables NTP authentication. The default setting is `disabled`. When authentication is enabled, the switch transmits NTP packets with the MAC address appended. **Command mode:** Global configuration
`ntp primary-key <1-65534>` Adds the NTP primary server key, which specifies which MD5 key is used by the primary server. **Command mode:** Global configuration
`ntp secondary-key <1-65534>` Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server. **Command mode:** Global configuration
`ntp trusted-key <1-65534>|0` Adds an MD5 key code to the list of trusted keys. Enter 0 (zero) to remove the selected key code. **Command mode:** Global configuration
`ntp enable` Enables the NTP synchronization service. **Command mode:** Global configuration
`no ntp enable` Disables the NTP synchronization service. **Command mode:** Global configuration
`show ntp` Displays the current NTP service settings. **Command mode:** All

NTP MD5 Key Commands

Table 86. NTP MD5 KEy Configuration Options

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

System SNMP Configuration

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

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

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

SNMP parameters that can be modified include:

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

Table 87. System SNMP Commands

Command Syntax and Usage
`snmp-server name <1-64 characters>` Configures the name for the system. The name can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server location <1-64 characters>` Configures the name of the system location. The location can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server contact <1-64 characters>` Configures the name of the system contact. The contact can have a maximum of 64 characters. **Command mode:** Global configuration
`snmp-server read-community <1-32 characters>` Configures the SNMP read community string. The read community string controls SNMP “get” access to the switch. It can have a maximum of 32 characters. The default read community string is *public*. **Command mode:** Global configuration

Table 87. System SNMP Commands

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

SNMPv3 Configuration

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

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

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

Table 88. SNMPv3 Configuration Commands

Command Syntax and Usage
`snmp-server user <1-16>` This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. **Command mode:** Global configuration To view command options, see page 145.
`snmp-server view <1-128>` This command allows you to create different MIB views. **Command mode:** Global configuration To view command options, see page 146.
`snmp-server access <1-32>` This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. **Command mode:** Global configuration To view command options, see page 147.
`snmp-server group <1-16>` A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. **Command mode:** Global configuration To view command options, see page 148.
`snmp-server community <1-16>` The community table contains objects for mapping community strings and version-independent SNMP message parameters. **Command mode:** Global configuration To view command options, see page 149.

Table 88. SNMPv3 Configuration Commands (continued)

`snmp-server target-address <1-16>` This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. **Command mode:** Global configuration To view command options, see page 150.
`snmp-server target-parameters <1-16>` This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. **Command mode:** Global configuration To view command options, see page 151.
`snmp-server notify <1-16>` A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. **Command mode:** Global configuration To view command options, see page 152.
`snmp-server version {v1v2v3|v3only}` This command allows you to enable or disable the access to SNMP versions 1, 2 or 3. The default value is `v1v2v3`. **Command mode:** Global configuration
`show snmp-server v3` Displays the current SNMPv3 configuration. **Command mode:** All

User Security Model Configuration

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

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

Table 89. User Security Model Configuration Commands

Command Syntax and Usage
`snmp-server user <1-16> name <1-32 characters>` This command allows you to configure a string that represents the name of the user. This is the login name that you need in order to access the switch. **Command mode:** Global configuration
`snmp-server user <1-16> authentication-protocol {md5|sha|none} authentication-password <password value>` This command allows you to configure the authentication protocol and password. The authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96 for compatibility mode, HMAC-SHA-96 for security strict mode, or none. The default algorithm is `none`. `MD5` authentication protocol is not available in security strict mode if you do not select SNMPv3 account backward compatibility. When you configure an authentication algorithm, you must provide a password, otherwise you will get an error message during validation. This command allows you to create or change your password for authentication. **Command mode:** Global configuration
`snmp-server user <1-16> privacy-protocol {aes|none} privacy-password <password value>` This command allows you to configure the type of privacy protocol and the privacy password. The privacy protocol protects messages from disclosure. The options are `aes` (AES-128 Advanced Encryption Standard Protocol) or `none`. If you specify `aes` as the privacy protocol, make sure that you have selected HMAC-SHA-256 authentication protocol. If you select `none` as the authentication protocol, you will get an error message. You can create or change the privacy password. **Command mode:** Global configuration
`no snmp-server user <1-16>` Deletes the USM user entries. **Command mode:** Global configuration
`show snmp-server v3 user <1-16>` Displays the USM user entries. **Command mode:** All

SNMPv3 View Configuration

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

Table 90. SNMPv3 View Configuration Commands

Command Syntax and Usage
`snmp-server view <1-128> name <1-32 characters>` This command defines the name for a family of view subtrees. **Command mode:** Global configuration
`snmp-server view <1-128> tree <1-64 characters>` This command defines MIB tree, which when combined with the corresponding mask defines a family of view subtrees. **Command mode:** Global configuration
`[no] snmp-server view <1-128> mask <1-32 characters>` This command defines the bit mask, which in combination with the corresponding tree defines a family of view subtrees. **Command mode:** Global configuration
`snmp-server view <1-128> type {included|excluded}` This command indicates whether the corresponding instances of `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyMask` define a family of view subtrees, which is included in or excluded from the MIB view. **Command mode:** Global configuration
`no snmp-server view <1-128>` Deletes the `vacmViewTreeFamily` group entry. **Command mode:** Global configuration
`show snmp-server v3 view <1-128>` Displays the current `vacmViewTreeFamily` configuration. **Command mode:** All

View-based Access Control Model Configuration

The view-based Access Control Model defines a set of services that an application can use for checking access rights of the user. Access control is needed when the user has to process SNMP retrieval or modification request from an SNMP entity.

Table 91. View-based Access Control Model Commands

Command Syntax and Usage
`snmp-server access <1-32> name <1-32 characters>` Defines the name of the group. **Command mode:** Global configuration
`snmp-server access <1-32> prefix <1-32 characters>` Defines the name of the context. An SNMP context is a collection of management information that an SNMP entity can access. An SNMP entity has access to many contexts. For more information on naming the management information, see RFC2571, the SNMP Architecture document. The view-based Access Control Model defines a table that lists the locally available contexts by contextName. **Command mode:** Global configuration
`snmp-server access <1-32> security {usm|snmpv1|snmpv2}` Allows you to select the security model to be used. **Command mode:** Global configuration
`snmp-server access <1-32> level {noAuthNoPriv|authNoPriv|authPriv}` Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
`snmp-server access <1-32> match {exact|prefix}` If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected. **Command mode:** Global configuration
`snmp-server access <1-32> read-view <1-32 characters>` Defines a read view name that allows you read access to a particular MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode:** Global configuration

Table 91. View-based Access Control Model Commands (continued)

Command Syntax and Usage
`snmp-server access <1-32> write-view <1-32 characters>` Defines a write view name that allows you write access to the MIB view. If the value is empty or if there is no active MIB view having this value then no access is granted. **Command mode:** Global configuration
`snmp-server access <1-32> notify-view <1-32 characters>` Defines a notify view name that allows you notify access to the MIB view. **Command mode:** Global configuration
`no snmp-server access <1-32>` Deletes the View-based Access Control entry. **Command mode:** Global configuration
`show snmp-server v3 access <1-32>` Displays the View-based Access Control configuration. **Command mode:** All

SNMPv3 Group Configuration

Table 92. SNMPv3 Group Configuration Commands

Command Syntax and Usage
`snmp-server group <1-16> security {usm|snmpv1|snmpv2}` Defines the security model. **Command mode:** Global configuration
`snmp-server group <1-16> user-name <1-32 characters>` Sets the user name as defined in the following command on page 145: `snmp-server user <1-16> name <1-32 characters>` **Command mode:** Global configuration
`snmp-server group <1-16> group-name <1-32 characters>` The name for the access group as defined in the following command: `snmp-server access <1-32> name <1-32 characters>` on page 145. **Command mode:** Global configuration
`no snmp-server group <1-16>` Deletes the `vacmSecurityToGroup` entry. **Command mode:** Global configuration
`show snmp-server v3 group <1-16>` Displays the current `vacmSecurityToGroup` configuration. **Command mode:** All

SNMPv3 Community Table Configuration

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

Table 93. SNMPv3 Community Table Configuration Commands

Command Syntax and Usage
`snmp-server community <1-16> index <1-32 characters>` Allows you to configure the unique index value of a row in this table. **Command string:** Global configuration
`snmp-server community <1-16> name <1-32 characters>` Defines the user name as defined in the following command on page 145: `snmp-server user <1-16> name <1-32 characters>` **Command string:** Global configuration
`snmp-server community <1-16> user-name <1-32 characters>` Defines a readable string that represents the corresponding value of an SNMP community name in a security model. **Command mode:** Global configuration
`snmp-server community <1-16> tag <1-255 characters>` Allows you to configure a tag. This tag specifies a set of transport endpoints to which a command responder application sends an SNMP trap. **Command mode:** Global configuration
`no snmp-server community <1-16>` Deletes the community table entry. **Command mode:** Global configuration
`show snmp-server v3 community <1-16>` Displays the community table configuration. **Command mode:** All

SNMPv3 Target Address Table Configuration

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

Table 94. Target Address Table Configuration Commands

Command Syntax and Usage
`snmp-server target-address <1-16> address <IP address> name <1-32 characters>` Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry. **Command mode:** Global configuration
`snmp-server target-address <1-16> name <1-32 characters> address <transport IP address>` Configures a transport IPv4 address that can be used in the generation of SNMP traps. **Command mode:** Global configuration
`snmp-server target-address <1-16> port <port number>` Allows you to configure a transport address port that can be used in the generation of SNMP traps. **Command mode:** Global configuration
`snmp-server target-address <1-16> taglist <1-255 characters>` Allows you to configure a list of tags that are used to select target addresses for a particular operation. **Command mode:** Global configuration
`snmp-server target-address <1-16> parameters-name <1-32 characters>` Defines the name as defined in the following command on page 151: `snmp-server target-parameters <1-16> name <1-32 characters>` **Command mode:** Global configuration
`no snmp-server target-address <1-16>` Deletes the Target Address Table entry. **Command mode:** Global configuration
`show snmp-server v3 target-address <1-16>` Displays the current Target Address Table configuration. **Command mode:** All

SNMPv3 Target Parameters Table Configuration

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

Table 95. Target Parameters Table Configuration Commands

Command Syntax and Usage
`snmp-server target-parameters <1-16> name <1-32 characters>` Allows you to configure the locally arbitrary, but unique, identifier that is associated with this entry. **Command mode:** Global configuration
`snmp-server target-parameters <1-16> message {snmpv1|snmpv2c|snmpv3}` Allows you to configure the message processing model that is used to generate SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters <1-16> security {usm|snmpv1|snmpv2}` Allows you to select the security model to be used when generating the SNMP messages. **Command mode:** Global configuration
`snmp-server target-parameters <1-16> user-name <1-32 characters>` Defines the name that identifies the user in the USM table (page 145) on whose behalf the SNMP messages are generated using this entry. **Command mode:** Global configuration
`snmp-server target-parameters <1-16> level {noAuthNoPriv|authNoPriv|authPriv}` Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol. **Command mode:** Global configuration
`no snmp-server target-parameters <1-16>` Deletes the `targetParamsTable` entry. **Command mode:** Global configuration
`show snmp-server v3 target-parameters <1-16>` Displays the current `targetParamsTable` configuration. **Command mode:** All

SNMPv3 Notify Table Configuration

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

Table 96. Notify Table Commands

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

System Access Configuration

The following table describes system access configuration commands.

Table 97. System Access Configuration Commands

Command Syntax and Usage
`access user user-password` Sets the user (`user`) password. The user has no direct responsibility for switch management. The user view switch status information and statistics, but cannot make any configuration changes. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Note:** To disable the user account, set the password to null (no password). **Command Mode**: Global configuration
`access user operator-password` Sets the operator (`oper`) password. The operator manages all functions of the switch. The operator can view all switch information and statistics and can reset ports. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. **Note:** To disable the operator account, set the password to null (no password). The default setting is disabled (no password). **Command Mode**: Global configuration
`access user administrator-password` Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the SI4093, including the ability to change both the user and administrator passwords. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Note:** You cannot disable the administrator password. **Command Mode**: Global configuration
`[no] access snmp {read-only|read-write}` Disables or provides read-only/write-read SNMP access. **Command mode:** Global configuration
`[no] access telnet enable` Enables or disables Telnet access. This command is disabled by default. **Command mode:** Global configuration
`[default] access telnet port [<`*1-65535*`>]` Sets an optional Telnet server port number for cases where the server listens for Telnet sessions on a non-standard port. **Command mode:** Global configuration

Table 97. System Access Configuration Commands (continued)

Command Syntax and Usage
[default] access tftp-port [<*1-65535*>] Sets the TFTP port for the switch. The default is port 69. **Command mode:** Global configuration
show access Displays the current system access parameters. **Command mode:** All

Management Network Configuration

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

Table 98. Management Network Configuration Commands

Command Syntax and Usage
access management-network <*mgmt network IPv4 or IPv6 address*> <*mgmt network mask or prefix length*> Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the IBM Networking OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network. **Command mode:** Global configuration
no access management-network <*mgmt network IPv4 or IPv6 address*> <*mgmt network mask or prefix length*> Removes a defined network, which consists of a management network address and a management network mask address. **Command mode:** Global configuration
access management-network <*mgmt network IPv4 address*> <*mgmt network mask*> {snmp-ro|snmp-rw} Adds a defined IPv4 network through which SNMP read-only or SNMP read/write switch access is allowed. Specify an IP address and mask address in dotted-decimal notation. **Command mode:** Global configuration
access management-network6 <*mgmt network IPv6 address*> <*IPv6 prefix length*> {snmp-ro|snmp-rw} Adds a defined IPv6 network through which SNMP read-only or SNMP read/write switch access is allowed. **Command mode:** Global configuration

Table 98. Management Network Configuration Commands

Command Syntax and Usage
`no access management-network {snmp-ro|snmp-rw}` Clears the IPv4 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
`no access management-network6 {snmp-ro|snmp-rw}` Clears the IPv6 SNMP read-only or SNMP read/write access control list for management purposes. **Command mode:** Global configuration
`show access management-network` Displays the current management network configuration and SNMP access management IP list. **Command mode:** All
`clear access management-network` Removes all defined management networks. **Command mode:** All except User EXEC

User Access Control Configuration

The following table describes user-access control commands.

Passwords can be a maximum of 128 characters.

Table 99. User Access Control Configuration Commands

Command Syntax and Usage
`access user` *<1-20>* Configures the User ID. **Command mode:** Global configuration
`access user eject` {*<user name>*|*<session ID>*} Ejects the specified user from the SI4093. **Command mode:** Global configuration
`clear line` *<1-12>* Ejects the user with the corresponding session ID from the SI4093. **Command mode:** Privileged EXEC
`access user user-password` *<1-128 characters>* Sets the user (`user`) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes. **Command mode:** Global configuration
`access user operator-password` *<1-128 characters>* Sets the operator (`oper`) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports. **Command mode:** Global configuration
`access user administrator-password` *<1-128 characters>* Sets the administrator (`admin`) password. The super user administrator has complete access to all information and configuration commands on the SI4093, including the ability to change both the user and administrator passwords. Access includes "`oper`" functions. **Command mode:** Global configuration
`show access user` Displays the current user status. **Command mode:** All

System User ID Configuration

The following table describes user ID configuration commands.

Table 100. User ID Configuration Commands

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

Strong Password Configuration

The following table describes strong password configuration commands.

Table 101. Strong Password Configuration Commands

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

Custom Daylight Saving Time Configuration

Use these commands to configure custom Daylight Saving Time. The DST is defined by two rules, the start rule and end rule. The rules specify the dates when the DST starts and finishes. These dates are represented as specific calendar dates or as relative offsets in a month (for example, 'the second Sunday of September').

Relative offset example:
2070901 = Second Sunday of September, at 1:00 a.m.

Calendar date example:
0070901 = September 7, at 1:00 a.m.

Table 102. Custom DST Configuration Commands

Command Syntax and Usage

`system custom-dst start-rule <WDDMMhh>`
Configures the start date for custom DST, as follows:
`WDMMhh`
W = week (0-5, where 0 means use the calender date)
D = day of the week (01-07, where 01 is Monday)
MM = month (1-12)
hh = hour (0-23)
Note: Week 5 is always considered to be the last week of the month.
Command mode: Global configuration

`system custom-dst end-rule <WDDMMhh>`
Configures the end date for custom DST, as follows:
`WDMMhh`
W = week (0-5, where 0 means use the calender date)
D = day of the week (01-07, where 01 is Monday)
MM = month (1-12)
hh = hour (0-23)
Note: Week 5 is always considered to be the last week of the month.
Command mode: Global configuration

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

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 168.

Table 103. Port Configuration Commands

Command Syntax and Usage
`interface port` <*port alias or number*> Enter Interface port mode. **Command mode:** Global configuration
`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
`description` <*1-64 characters*> Sets a description for the port. The assigned port name appears next to the port description on some information and statistics screens. The default is set to the port number. **Command mode:** Interface port
`switchport mode {access|trunk|private-vlan}` Configures the port's trunking mode: – `access` allows association to a single VLAN – `trunk` allows association to multiple VLANs – `private-vlan` allows association to a private VLAN Default mode is `access`. **Note**: When switching from access to trunk mode, the port inherits the access VLAN as the trunk Native-VLAN. **Note**: When switching from trunk to access mode, the port inherits the trunk Native-VLAN as the access VLAN. **Command mode:** Interface port/Interface portchannel
`switchport access vlan` <*1-4094*> Configures the associated VLAN used in access mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel

Table 103. Port Configuration Commands (continued)

Command Syntax and Usage
`no switchport access vlan` Resets the access VLAN to its default value. **Command mode:** Interface port/Interface portchannel
`switchport trunk native vlan` <*1-4094*> Configures the Port VLAN ID (PVID) or Native-VLAN used to carry untagged traffic in trunk mode. If the VLAN does not exist, it will be created and enabled automatically. Default value is 1 for data ports and 4095 for the management port. **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan [add|remove]` <*VLAN ID range*> Updates the associated VLANs in trunk mode.If any VLAN in the range does not exist, it will be created and enabled automatically. – `add` enables the VLAN range in addition to the current configuration – `remove` eliminates the VLAN range from the current configuration **Command mode:** Interface port/Interface portchannel
`switchport trunk allowed vlan {all|none}` – `all` associates all existing and enabled VLANs to the port. This is an operational command applicable only to VLANs currently configured at the moment of execution. VLANs created afterward will not be associated automatically. Also, as an operational command, it will not be dumped into the configuration file. – `none` removes the port from all currently associated VLANS except the default VLAN **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan mapping` <*primary VLAN*> Enables or disables a private VLAN promiscuous port to/from a primary VLAN. **Command mode:** Interface port/Interface portchannel
`[no] switchport private-vlan host-association` <*primary VLAN*> <*secondary VLAN*> Adds or removes a private VLAN host port to/from a secondary VLAN. **Command mode:** Interface port/Interface portchannel
`[no] vlan dot1q tag native` Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed at egress from packets whose VLAN tag matches the port PVID/Native-vlan. The default setting is `disabled`. **Note:** In global configuration mode, this is an operational command used to set the VLAN tag persistence on all ports currently tagged at the moment of execution. VLAN tag persistence will not be set automatically for ports tagged afterward. Also, as an operational command, it will not be dumped into the configuration file. **Command mode:** Global configuration/Interface port/Interface portchannel

Table 103. Port Configuration Commands (continued)

Command Syntax and Usage
[no] tagpvid-ingress Enables or disables tagging the ingress frames with the port's VLAN ID. When enabled, the PVID tag is inserted into untagged and 802.1Q single-tagged ingress frames as outer VLAN ID. The default setting is disabled. **Command mode**: Interface port/Interface portchannel
[no] flood-blocking Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port. **Command mode:** Interface port
[no] mac-address-table mac-notification Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table. **Command mode:** Global configuration
[no] learning Enables or disables FDB learning on the port. **Command mode:** Interface port
port-channel min-links <*1-32*> Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the down state. **Command mode:** Interface port
[no] storm-control broadcast level pps <*0-2097151*> Limits the number of broadcast packets per second to the specified value. If disabled, the port forwards all broadcast packets. **Command mode:** Interface port
[no] storm-control multicast level pps <*0-2097151*> Limits the number of multicast packets per second to the specified value. If disabled, the port forwards all multicast packets. **Command mode:** Interface port
[no] storm-control unicast level pps <*0-2097151*> Limits the number of unknown unicast packets per second to the specified value. If disabled, the port forwards all unknown unicast packets. **Command mode:** Interface port
no shutdown Enables the port. **Command mode:** Interface port

Table 103. Port Configuration Commands (continued)

Command Syntax and Usage
`shutdown` Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 164.) **Command mode:** Interface port
`show interface port` <*port alias or number*> Displays current port parameters. **Command mode:** All

Port Error Disable and Recovery Configuration

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

Table 104. Port Error Disable Commands

Command Syntax and Usage
`errdisable recovery` Enables automatic error-recovery for the port. The default setting is `enabled`. **Note**: Error-recovery must be enabled globally before port-level commands become active. **Command mode:** Interface port
`no errdisable recovery` Enables automatic error-recovery for the port. **Command mode:** Interface port
`show interface port` <*port alias or number*> `errdisable` Displays current port Error Disable parameters. **Command mode:** All

Port Link Configuration

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

Table 105. Port Link Configuration Commands

Command Syntax and Usage
`speed {1000|10000|auto}` Sets the link speed. Some options are not valid on all ports. The choices include: – 1000 Mbps – 10000 Mps – any (auto negotiate port speed) **Command mode:** Interface port
`duplex {full|half|auto}` Sets the operating mode. The choices include: – Auto negotiation (default) – Half-duplex – Full-duplex **Command mode:** Interface port
`flowcontrol receive {on|off}` Enables or disables flow control receive. **Note**: For external ports (EXT*x*) the default setting is no flow control, and for internal ports (INT*x*) the default setting is both receive and transmit. **Command mode:** Interface port
`flowcontrol send {on|off}` Enables or disables flow control transmit. **Note**: For external ports (EXT*x*) the default setting is no flow control, and for internal ports (INT*x*) the default setting is both receive and transmit. **Command mode:** Interface port
`[no] auto` Turns auto-negotiation on or off. **Command mode:** Interface port
`show interface port <`*port alias or number*`>` Displays current port parameters. **Command mode:** All

Temporarily Disabling a Port

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

```
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 (SIM) is reset. See the “Operations Commands” on page 253 for other operations-level commands.

Unidirectional Link Detection Configuration

UDLD commands are described in the following table.

Table 106. Port UDLD Configuration Commands

Command Syntax and Usage
`[no] udld` Enables or disables UDLD on the port. **Command mode:** Interface port
`[no] udld aggressive` Configures the UDLD mode for the selected port, as follows: – **Normal**: Detect unidirectional links that have mis-connected interfaces. The port is disabled if UDLD determines that the port is mis-connected. Use the “no” form to select normal operation. – **Aggressive**: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds. **Command mode:** Interface port
`show interface port <`*port number*`> udld` Displays current port UDLD parameters. **Command mode:** All

Port OAM Configuration

Operation, Administration, and Maintenance (OAM) protocol allows the switch to detect faults on the physical port links. OAM is described in the IEEE 802.3ah standard. OAM Discovery commands are described in the following table.

Table 107. Port OAM Configuration Commands

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

Port ACL Configuration

The following table describes port ACL configuration commands

Table 108. Port ACL/QoS Configuration Commands

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

Port 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 170.

Table 109. Port WRED Options

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

Port WRED Transmit Queue Configuration

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

Table 110. Port WRED Transmit Queue Options

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

Table 110. Port WRED Transmit Queue Options

Command Syntax and Usage
`random-detect transmit-queue <0-7> enable` Sets the WRED transmit queue configuration to `on`. **Command mode:** Interface port
`no random-detect transmit-queue <0-7> enable` Sets the WRED transmit queue configuration to `off`. **Command mode:** Interface port

Management Port Configuration

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

Table 111. Management Port Configuration Commands

Command Syntax and Usage
`speed {10|100|1000|auto}` Sets the link speed. The choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – Auto — for auto negotiation **Command mode:** Interface port
`duplex {full|half|auto}` Sets the operating mode. The choices include: – Full-duplex – Half-duplex – Auto — for auto negotiation (default) **Command mode:** Interface port
`flowcontrol {receive|send} {on|off}` Activates or deactivates one type of flow control. The choices include: – Receive flow control – Transmit flow control **Command mode:** Interface port
`no flowcontrol` Deactivates flow control globally.
`no shutdown` Enables the port. **Command mode:** Interface port

Table 111. Management Port Configuration Commands (continued)

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

Quality of Service Configuration

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

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 112. CoPP Commands

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

Weighted Random Early Detection Configuration

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

These commands allow you to configure global WRED parameters. For port WRED commands, see "Port WRED Configuration" on page 167.

Table 113. WRED Configuration Options

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

Table 113. WRED Configuration Options

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

WRED Transmit Queue Configuration

Table 114. WRED Transmit Queue Options

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

Access Control Configuration

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

For information about assigning ACLs to ports, see “Port ACL Configuration” on page 166.

Table 115. General ACL Configuration Commands

Command Syntax and Usage
[no] `access-control list` *<1-640>* Configures an Access Control List. **Command mode:** Global configuration To view command options, see page 173.
[no] `access-control group` *<1-640>* Configures an ACL Group. **Command mode:** Global configuration To view command options, see page 185.
`show access-control` Displays the current ACL parameters. **Command mode:** All

Access Control List Configuration

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

Table 116. ACL Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-640*> egress-port port <*port alias or number*> Configures the ACL to function on egress packets. **Command mode:** Global configuration
access-control list <*1-640*> action {permit|deny|set-priority <*0-7*>} Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7). **Command mode:** Global configuration
[no] access-control list <*1-640*> statistics Enables or disables the statistics collection for the Access Control List. **Command mode:** Global configuration
default access-control list <*1-640*> Resets the ACL parameters to their default values. **Command mode:** Global configuration
show access-control list <*1-640*> Displays the current ACL parameters. **Command mode:** All
[no] access-control list6 <*1-128*> Configures an IPv6 Access Control List. To view command options, see page 177. **Command mode:** Global configuration

Ethernet Filtering Configuration

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

Table 117. Ethernet Filtering Configuration Commands

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

IPv4 Filtering Configuration

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

Table 118. IP version 4 Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-640*> ipv4 source-ip-address <*IP address*> <*IP mask*> Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation. **Command mode:** Global configuration
[no] access-control list <*1-640*> ipv4 destination-ip-address <*IP address*> <*IP mask*> Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL. **Command mode:** Global configuration
[no] access-control list <*1-640*> ipv4 protocol <*0-255*> Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp **Command mode:** Global configuration
[no] access-control list <*1-640*> ipv4 type-of-service <*0-255*> Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349. **Command mode:** Global configuration
default access-control list <*1-640*> ipv4 Resets the IPv4 parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-640*> ipv4 Displays the current IPv4 parameters. **Command mode:** All

TCP/UDP Filtering Configuration

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

Table 119. TCP/UDP Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-640*> tcp-udp source-port <*1-65535*> <*mask (0xFFFF)*> Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports: **Number** **Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
[no] access-control list <*1-640*> tcp-udp destination-port <*1-65535*> <*mask (0xFFFF)*> Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with sport above. **Command mode:** Global configuration
[no] access-control list <*1-640*> tcp-udp flags <*value (0x0-0x3f)*> <*mask (0x0-0x3f)*> Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration
default access-control list <*1-640*> tcp-udp Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-640*> tcp-udp Displays the current TCP/UDP Filtering parameters. **Command mode:** All

Packet Format Filtering Configuration

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

Table 120. Packet Format Filtering Configuration Commands

Command Syntax and Usage
[no] access-control list <*1-640*> packet-format ethernet {ethertype2| snap|llc} Defines the Ethernet format for the ACL. **Command mode:** Global configuration
[no] access-control list <*1-640*> packet-format tagging {any|none|tagged} Defines the tagging format for the ACL. **Command mode:** Global configuration
[no] access-control list <*1-640*> packet-format ip {ipv4|ipv6} Defines the IP format for the ACL. **Command mode:** Global configuration
default access-control list <*1-640*> packet-format Resets Packet Format parameters for the ACL to their default values. **Command mode:** Global configuration
show access-control list <*1-640*> packet-format Displays the current Packet Format parameters for the ACL. **Command mode:** All

ACL IPv6 Configuration

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

Table 121. IPv6 ACL Options

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

Table 121. IPv6 ACL Options

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

IPv6 Filtering Configuration

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

Table 122. IP version 6 Filtering Options

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

Table 122. IP version 6 Filtering Options

Command Syntax and Usage
`default access-control list6 <1-128> ipv6` Resets the IPv6 parameters for the ACL to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128> ipv6` Displays the current IPv6 parameters. **Command mode:** All

IPv6 TCP/UDP Filtering Configuration

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

Table 123. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
[no] `access-control list6 <1-128> tcp-udp source-port <1-65535> <mask (0xFFFF)>` Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed here are some of the well-known ports: **Number Name** 20 ftp-data 21 ftp 22 ssh 23 telnet 25 smtp 37 time 42 name 43 whois 53 domain 69 tftp 70 gopher 79 finger 80 http **Command mode:** Global configuration
[no] `access-control list6 <1-128> tcp-udp destination-port <1-65535> <mask (0xFFFF)>` Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above. **Command mode:** Global configuration
[no] `access-control list6 <1-128> tcp-udp flags <value (0x0-0x3f)> <mask (0x0-0x3f)>` Defines a TCP/UDP flag for the ACL. **Command mode:** Global configuration

Table 123. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
`default access-control list6 <1-128> tcp-udp` Resets the TCP/UDP parameters for the ACL to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128> tcp-udp` Displays the current TCP/UDP Filtering parameters. **Command mode:** All

IPv6 Re-Marking Configuration

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

IPv6 Re-Mark In-Profile Configuration

Table 124. IPv6 Re-Marking In-Profile Options

Command Syntax and Usage
`[no] access-control list6 <1-128> re-mark dot1p <0-7>` Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`[no] access-control list6 <1-128> re-mark in-profile dscp <0-63>` Re-marks the DSCP value for in-profile traffic. **Command mode:** Global configuration
`[no] access-control list6 <1-128> re-mark use-tos-precedence` Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`default access-control list6 <1-128> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128> re-mark` Displays current re-mark parameters. **Command mode:** All

VMAP Configuration

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

For more information about VLAN Map configuration commands, see "Access Control List Configuration" on page 173.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration" on page 207.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 237.

Table 125 lists the general VMAP configuration commands.

Table 125. VMAP Configuration Commands

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

Table 125. VMAP Configuration Commands (continued)

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

Table 125. VMAP Configuration Commands (continued)

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

Table 125. VMAP Configuration Commands (continued)

Command Syntax and Usage
`access-control vmap <1-128> packet-format tagging any|none|tagged` Sets filtering based on packet tagging. The options are: – `any`: Filter tagged & untagged packets – `none`: Filter only untagged packets – `tagged`: Filter only tagged packets **Command mode:** Global configuration
`no access-control vmap <1-128> packet-format ethernet|ip|tagging` Disables filtering based on the specified packet format. **Command mode:** Global configuration
`access-control vmap <1-128> re-mark dot1p <0-7>` Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
`no access-control vmap <1-128> re-mark dot1p` Disables the use of dot1p for in-profile traffic ACL re-mark configuration. **Command mode:** Global configuration
`access-control vmap <1-128> re-mark in-profile|out-profile dscp <0-63>` Sets the ACL re-mark configuration user update priority. **Command mode:** Global configuration
`no access-control vmap <1-128> re-mark in-profile|out-profile` Removes all re-mark in-profile or out-profile settings. **Command mode:** Global configuration
`[no] access-control vmap <1-128> re-mark use-tos-precedence` Enables or disables the use of the TOS precedence for in-profile traffic. **Command mode:** Global configuration
`[no] access-control vmap <1-128> statistics` Enables or disables the statistics collection for the VMAP. **Command mode:** Global configuration
`access-control vmap <1-128> tcp-udp source-port|destination-port <1-65535> <port mask (0x0001 - 0xFFFF)>` Sets the TCP/UDP filtering source port or destination port and port mask for this ACL. **Command mode:** Global configuration
`access-control vmap <1-128> tcp-udp flags [<flags mask (0x0-0x3F)>]` Sets the TCP flags for this ACL. **Command mode:** Global configuration

Table 125. VMAP Configuration Commands (continued)

Command Syntax and Usage
`no access-control vmap <1-128> tcp-udp` Removes TCP/UDP filtering for this ACL. **Command mode:** Global configuration
`default access-control vmap <1-128>` Resets the VMAP parameters to their default values. **Command mode:** Global configuration
`show access-control vmap <1-128>` Displays the current VMAP parameters. **Command mode:** All

ACL Group Configuration

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

Table 126. ACL Group Configuration Commands

Command Syntax and Usage
`access-control group <1-640> list <1-640>` Adds the selected ACL to the ACL group. **Command mode:** Global configuration
`no access-control group <1-640> list <1-640>` Removes the selected ACL from the ACL group. **Command mode:** Global configuration
`show access-control group <1-640>` Displays the current ACL group parameters. **Command mode:** All

ACL Metering Configuration

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

Table 127. ACL Metering Configuration Commands

Command Syntax and Usage
`access-control list <1-640> meter committed-rate <64-10000000>` Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64. **Command mode:** Global configuration
`access-control list <1-640> meter maximum-burst-size <32-4096>` Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096 **Command mode:** Global configuration
[no] `access-control list <1-640> meter enable` Enables or disables ACL Metering. **Command mode:** Global configuration
`access-control list <1-640> meter action {drop|pass}` Configures the ACL meter to either drop or pass out-of-profile traffic. **Command mode:** Global configuration
`default access-control list <1-640> meter` Sets the ACL meter configuration to its default values. **Command mode:** Global configuration
`[no] access-control list <1-640> meter log` Configures the ACL meter to log out-of-profile notifications. **Command mode:** Global configuration
`no access-control list <1-640> meter` Deletes the selected ACL meter. **Command mode:** Global configuration
`show access-control list <1-640> meter` Displays current ACL Metering parameters. **Command mode:** All

ACL Re-Mark Configuration

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

Table 128. ACL Re-Marking Configuration Commands

Command Syntax and Usage
`access-control list <1-640> re-mark dot1p <0-7>` Defines 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`no access-control list <1-640> re-mark dot1p` Disables use of 802.1p value for re-marked packets. **Command mode:** Global configuration
`[no] access-control list <1-640> re-mark use-tos-precedence` Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`default access-control list <1-640> re-mark` Sets the ACL Re-mark configuration to its default values. **Command mode:** Global configuration
`show access-control list <1-640> re-mark` Displays current Re-mark parameters. **Command mode:** All

Re-Marking In-Profile Configuration

Table 129. ACL Re-Mark In-Profile Commands

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

Re-Marking Out-of-Profile Configuration

Table 130. ACL Re-Mark Out-of-Profile Commands

Command Syntax and Usage
`access-control list <1-640> re-mark out-profile dscp <0-63>` Sets the DiffServ Code Point (DSCP) of out-of-profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets. **Command mode:** Global configuration
`no access-control list <1-640> re-mark out-profile dscp` Disables use of DSCP value for out-of-profile traffic. **Command mode:** Global configuration
`show access-control list <1-640> re-mark` Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking Configuration

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

Table 131. IPv6 General Re-Mark Options

Command Syntax and Usage
`[no] access-control list6 <1-128> re-mark dot1p <0-7>` Re-marks the 802.1p value. The value is the priority bits information in the packet structure. **Command mode:** Global configuration
`[no] no access-control list6 <1-128> re-mark use-tos-precedence` Enables or disables mapping of TOS (Type of Service) priority to 802.1p priority for in-profile packets. When enabled, the TOS value is used to set the 802.1p value. **Command mode:** Global configuration
`default access-control list6 <1-128> re-mark` Sets the ACL re-mark parameters to their default values. **Command mode:** Global configuration
`show access-control list6 <1-128> re-mark` Displays current re-mark parameters. **Command mode:** All

IPv6 Re-Marking In-Profile Configuration

Table 132. IPv6 Re-Mark In-Profile Options

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

Layer 2 Configuration

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

Table 133. Layer 2 Configuration Commands

Command Syntax and Usage
`show layer2` Displays current Layer 2 parameters. **Command mode:** All

Forwarding Database Configuration

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

Table 134. FDB Configuration Commands

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

Static Multicast MAC Configuration

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

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

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

Table 135. Static Multicast MAC Configuration Commands

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

Static FDB Configuration

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

Table 136. FDB Configuration Commands

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

LLDP Configuration

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

Table 137. LLDP Configuration Commands

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

Table 137. LLDP Configuration Commands

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

LLDP Port Configuration

Use the following commands to configure LLDP port options.

Table 138. LLDP Port Commands

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

Table 138. LLDP Port Commands

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

LLDP Optional TLV configuration

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

Table 139. 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 139. Optional TLV Commands (continued)

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

Trunk Configuration

Trunk groups can provide super-bandwidth connections between SI4093 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 SI4093, 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 140. Trunk Configuration Commands

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

IP Trunk Hash Configuration

Use the following commands to configure IP trunk hash settings for the 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 141 combined with the hash parameters listed in Table 142.

Table 141. Trunk Hash Settings

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

Layer 2 Trunk Hash

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

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

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

Table 142. Layer 2 Trunk Hash Options

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

Table 142. Layer 2 Trunk Hash Options (continued)

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

Layer 3 Trunk Hash

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

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

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

Table 143. Layer 3 Trunk Hash Options

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

Link Aggregation Control Protocol Configuration

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

Table 144. Link Aggregation Control Protocol Commands

Command Syntax and Usage
`lacp system-priority <1-65535>` Defines the priority value for the SI4093. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Global configuration
`lacp timeout {short|long}` Defines the timeout period before invalidating LACP data from a remote partner. Choose `short` (3 seconds) or `long` (90 seconds). The default value is `long`. **Note:** It is recommended that you use a timeout value of `long`, to reduce LACPDU processing. If your SI4093's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP. **Command mode:** Global configuration
`default lacp [system-priority|timeout]` Restores either the VFSM priority value, timeout period or both to their default values. **Command mode:** Global configuration
`no lacp <1-65535>` Deletes a selected LACP trunk, based on its *admin key*. This command is equivalent to disabling LACP on each of the ports configured with the same *admin key*. **Command mode:** Global configuration
`portchannel <trunk ID> lacp key <1-65535>` Enables a static LACP trunk. In this mode, ports sharing the same LACP admin key can form a single trunk, with the specified `trunk ID`. The active trunk is picked based on the ports which occupy first the trunk ID. Member ports that cannot join this trunk are prohibited from forming secondary LACP groups. Instead, they are set in a suspend state where they discard all non-LACP traffic. **Command mode:** Global configuration
`no portchannel <trunk ID>` Disables a static LACP trunk. **Command mode:** Global configuration
`show lacp` Display current LACP configuration. **Command mode:** All

LACP Port Configuration

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

Table 145. Link Aggregation Control Protocol Commands

Command Syntax and Usage
`lacp mode {off|active|passive}` Set the LACP mode for this port, as follows: – **off** Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is `off`. – **active** Turn LACP on and set this port to active. Active ports initiate LACPDUs. – **passive** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports. **Command mode:** Interface port
`lacp priority <1-65535>` Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768. **Command mode:** Interface port
`lacp key <1-65535>` Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group. **Command mode:** Interface port
`port-channel min-links <1->` Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the `down` state. **Command mode:** Interface port
`default lacp [key | mode | priority]` Restores the selected parameters to their default values. **Command mode:** Interface port
`show interface port <port alias or number> lacp` Displays the current LACP configuration for this port. **Command mode:** All

Layer 2 Failover Configuration

Use these commands to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the *IBM Networking OS Application Guide*.

Table 146. Layer 2 Failover Configuration Commands

Command Syntax and Usage
`failover enable` Globally turns Layer 2 Failover `on`. **Command mode:** Global configuration
`no failover enable` Globally turns Layer 2 Failover `off`. **Command mode:** Global configuration
`show failover trigger` Displays current Layer 2 Failover parameters. **Command mode:** All

Failover Trigger Configuration

Table 147. Failover Trigger Configuration Commands

Command Syntax and Usage
[no] `failover trigger <`*1-8*`> enable` Enables or disables the Failover trigger. **Command mode:** Global configuration
`no failover trigger <`*1-8*`>` Deletes the Failover trigger. **Command mode:** Global configuration
`failover trigger <`*1-8*`> limit <`*0-1024*`>` Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational. **Command mode:** Global configuration
`show failover trigger <`*1-8*`>` Displays the current failover trigger settings. **Command mode:** All

Auto Monitor Configuration

Table 148. Auto Monitor Configuration Commands

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

Failover Manual Monitor Port Configuration

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

Note: AMON and MMON configurations are mutually exclusive.

Table 149. Failover Manual Monitor Port Commands

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

Failover Manual Monitor Control Configuration

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

Table 150. Failover Manual Monitor Control Commands

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

VLAN Configuration

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

Internal server ports and external uplink ports are members of SPAR VLAN 4081-4083 by default. Up to 4094 VLANs can be configured on the SI4093.

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

Table 151. VLAN Configuration Commands

Command Syntax and Usage
`vlan` <*VLAN number*> Enter VLAN configuration mode. **Command mode:** Global configuration
`name` <*1-32 characters*> Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one. **Command mode:** VLAN
`[no] shutdown` Disables or enables local traffic on the specified VLAN. Default setting is enabled (`no shutdown`) **Command mode:** VLAN
`[no] vmap` <*1-128*> `[extports|intports]` Adds or removes a VLAN Map to the VLAN membership. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VLAN. **Command mode:** VLAN
`[no] management` Configures this VLAN as a management VLAN. You must have at least one internal port in each new management VLAN. Management port (MGT1) is automatically added to management VLAN. **Command mode:** VLAN
`[no] flood` Configures the switch to flood unregistered IP multicast traffic to all ports. The default setting is `enabled`. **Note:** If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group. **Command mode:** VLAN

Table 151. VLAN Configuration Commands (continued)

Command Syntax and Usage
`[no] cpu` Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table, as follows: – If no Mrouter is present, drop subsequent packets with same IPMC. – If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is `enabled`. **Note**: If both `flood` and `cpu` are disabled, then the switch drops all unregistered IPMC traffic. **Command mode:** VLAN
`[no] optflood` Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is `disabled`. **Command mode:** VLAN
`show vlan information` Displays the current VLAN configuration. **Command mode:** All

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

Private VLAN Configuration

Use the following commands to configure Private VLAN.

Table 152. Private VLAN Configuration Commands

Command Syntax and Usage
`[no] private-vlan primary` Enables or disables the VLAN type as a Primary VLAN. A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN. **Command mode:** VLAN
`[no] private-vlan community` Enables or disables the VLAN type as a community VLAN. Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs. **Command mode:** VLAN
`[no] private-vlan isolated` Enables or disables the VLAN type as an isolated VLAN. The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. **Command mode:** VLAN
`private-vlan association [add|remove]` <*secondary VLAN list*> Configures Private VLAN mapping between a primary VLAN and secondary VLANs. Enter the primary VLAN ID. If no optional parameter is specified, the list of secondary VLANs, replaces the currently associated secondary VLANs. Otherwise: – `add` appends the secondary VLANs to the ones currently associated – `remove` excludes the secondary VLANs from the ones currently associated **Command mode:** VLAN
`show vlan private-vlan [`<*2-4094*>`]` Displays current parameters for the selected Private VLAN(s). **Command mode:** VLAN

Layer 3 Configuration

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

Table 153. Layer 3 Configuration Commands

Command Syntax and Usage
`interface ip <`*interface number*`>` Configures the IP Interface. The SI4093 supports up to 4 IP interfaces.To view command options, see page 211. **Command mode:** Global configuration
`show layer3` Displays the current IP configuration. **Command mode:** All

IP Interface Configuration

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

IP Interfaces 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 154. IP Interface Configuration Commands

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

Table 154. IP Interface Configuration Commands (continued)

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

Default Gateway Configuration

The switch can be configured with up to 4 IPv4 gateways. Gateways 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 155. Default Gateway Configuration Commands

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

Network Filter Configuration

Table 156. IP Network Filter Configuration Commands

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

IGMP Configuration

Table 157 describes the commands used to configure basic IGMP parameters.

Table 157. IGMP Configuration Commands

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

The following sections describe the IGMP configuration options.

IGMP Snooping Configuration

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

Table 158 describes the commands used to configure IGMP Snooping.

Table 158. IGMP Snooping Configuration Commands

Command Syntax and Usage
`ip igmp snoop mrouter-timeout <1-600>` Configures the timeout value for IGMP Membership Queries (mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds. **Command mode:** Global configuration
`ip igmp snoop source-ip <IP address>` Configures the source IP address used as a proxy for IGMP Group Specific Queries. **Command mode:** Global configuration
`ip igmp snoop vlan <VLAN number>` Adds the selected VLAN(s) to IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop vlan <VLAN number>` Removes the selected VLAN(s) from IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop vlan all` Removes all VLANs from IGMP Snooping. **Command mode:** Global configuration
`ip igmp snoop enable` Enables IGMP Snooping. **Command mode:** Global configuration
`no ip igmp snoop enable` Disables IGMP Snooping. **Command mode:** Global configuration
`show ip igmp snoop` Displays the current IGMP Snooping parameters. **Command mode:** All

IGMPv3 Configuration

Table 159 describes the commands used to configure IGMP version 3.

Table 159. IGMP version 3 Configuration Commands

Command Syntax and Usage
`ip igmp snoop igmpv3 sources <1-64>` Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 v1v2` Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is `enabled`. **Command mode:** Global configuration
`[no] ip igmp snoop igmpv3 exclude` Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is `enabled`. **Command mode:** Global configuration
`ip igmp snoop igmpv3 enable` Enables IGMP version 3. The default value is `disabled`. **Command mode:** Global configuration
`no ip igmp snoop igmpv3 enable` Disables IGMP version 3. **Command mode:** Global configuration
`show ip igmp snoop igmpv3` Displays the current IGMP v3 Snooping configuration. **Command mode:** All

IGMP Static Multicast Router Configuration

Table 160 describes the commands used to configure a static multicast router.

Note: When static Mrouters are used, the switch continues learning dynamic Mrouters via IGMP snooping. However, dynamic Mrouters may not replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table 160. IGMP Static Multicast Router Configuration Commands

Command Syntax and Usage
`ip igmp mrouter` *<port alias or number> <VLAN number> <version (1-3)>* Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2 or 3) of the multicast router. **Command mode:** Global configuration
`no ip igmp mrouter` *<port alias or number> <VLAN number> <version (1-3)>* Removes a static multicast router from the selected port/VLAN combination. **Command mode:** Global configuration
`no ip igmp mrouter all` Removes all static multicast routers. **Command mode:** Global configuration
`clear ip igmp mrouter` Clears the Dynamic router port table. **Command mode:** Global configuration
`show ip igmp mrouter` Displays the current IGMP Static Multicast Router parameters. **Command mode:** All

IGMP Filtering Configuration

Table 161 describes the commands used to configure an IGMP filter.

Table 161. IGMP Filtering Configuration Commands

Command Syntax and Usage
`ip igmp profile <1-16>` Configures the IGMP filter. To view command options, see page 220. **Command mode:** Global configuration
`ip igmp filtering` Enables IGMP filtering globally. **Command mode:** Global configuration
`no ip igmp filtering` Disables IGMP filtering globally. **Command mode:** Global configuration
`show ip igmp filtering` Displays the current IGMP Filtering parameters. **Command mode:** All

IGMP Filter Definition

Table 162 describes the commands used to define an IGMP filter.

Table 162. IGMP Filter Definition Commands

Command Syntax and Usage
`ip igmp profile` <*1-16*> `range` <*IP address 1*> <*IP address 2*> Configures the range of IP multicast addresses for this filter. **Command mode:** Global configuration
`ip igmp profile` <*1-16*> `action` {`allow`|`deny`} Allows or denies multicast traffic for the IP multicast addresses specified. The default action is `deny`. **Command mode:** Global configuration
`ip igmp profile` <*1-16*> `enable` Enables this IGMP filter. **Command mode:** Global configuration
`no ip igmp profile` <*1-16*> `enable` Disables this IGMP filter. **Command mode:** Global configuration
`no ip igmp profile` <*1-16*> Deletes this filter's parameter definitions. **Command mode:** Global configuration
`show ip igmp profile` <*1-16*> Displays the current IGMP filter. **Command mode:** All

IGMP Filtering Port Configuration

Table 163 describes the commands used to configure a port for IGMP filtering.

Table 163. IGMP Filter Port Configuration Commands

Command Syntax and Usage
`[no] ip igmp filtering` Enables or disables IGMP filtering on this port. **Command mode:** Interface port
`ip igmp profile <1-16>` Adds an IGMP filter to this port. **Command mode:** Interface port
`no ip igmp profile <1-16>` Removes an IGMP filter from this port. **Command mode:** Interface port
`show interface port <port alias or number> igmp-filtering` Displays the current IGMP filter parameters for this port. **Command mode:** All

IGMP Advanced Configuration

Table 164 describes the commands used to configure advanced IGMP parameters.

Table 164. IGMP Advanced Configuration Commands

Command Syntax and Usage
`ip igmp query-interval <1-600>` Sets the IGMP router query interval, in seconds. The default value is 125. **Command mode:** Global configuration
`ip igmp robust <1-10>` Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If you expect the subnet to have a high rate of packet loss, increase the value. The default value is 2. **Command mode:** Global configuration
`ip igmp timeout <1-255>` Configures the Query Response Interval. This is a value used to determine the Group Membership Interval, together with the Robustness Variable and the Query Interval. The range is from 1 to 255 seconds.The default is 10 seconds. **Command mode:** Global configuration
`[no] ip igmp fastleave <VLAN number>` Enables or disables Fastleave processing. Fastleave lets the switch immediately remove a port from the IGMP port list if the host sends a Leave message and the proper conditions are met. This command is disabled by default. **Command mode:** Global configuration
`[no] ip igmp rtralert` Enables or disables the Router Alert option in IGMP messages. **Command mode:** Global configuration

Domain Name System Configuration

The Domain Name System (DNS) commands are used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

Table 165. Domain Name Service Commands

Command Syntax and Usage
[no] `ip dns primary-server` <*IP address*> You are prompted to set the IPv4 address for your primary DNS server, using dotted decimal notation. **Command mode:** Global configuration
[no] `ip dns secondary-server` <*IP address*> You are prompted to set the IPv4 address for your secondary DNS server, using dotted decimal notation. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
[no] `ip dns ipv6 primary-server` <*IP address*> You are prompted to set the IPv6 address for your primary DNS server, using hexadecimal format with colons. **Command mode:** Global configuration
[no] `ip dns ipv6 secondary-server` <*IP address*> You are prompted to set the IPv6 address for your secondary DNS server, using hexadecimal format with colons. If the primary DNS server fails, the configured secondary will be used instead. **Command mode:** Global configuration
`ip dns ipv6 request-version {ipv4|ipv6}` Sets the protocol used for the first request to the DNS server, as follows: – IPv4 – IPv6 **Command mode:** Global configuration
[no] `ip dns domain-name` <*string*> Sets the default domain name used by the switch. For example: `mycompany.com` **Command mode:** Global configuration
`show ip dns` Displays the current Domain Name System settings. **Command mode:** All

IPv6 Default Gateway Configuration

The switch supports IPv6 default gateways.

- Gateway 132 is reserved for management.

Table 166 describes the IPv6 Default Gateway Configuration commands.

Table 166. IPv6 Default Gateway Configuration Commands

Command Syntax and Usage
`ip gateway6 {<gateway number>} address <IPv6 address>` Configures the IPv6 address of the default gateway, in hexadecimal format with colons (such as 3001:0:0:0:0:0:abcd:12). **Command mode**: Global configuration
`[no] ip gateway6 {<gateway number>} enable` Enables or disables the default gateway. **Command mode**: Global configuration
`no ip gateway6 {<gateway number>}` Deletes the default gateway. **Command mode**: Global configuration
`show ipv6 gateway6 {<gateway number>}` Displays the current IPv6 default gateway configuration. **Command mode**: All

IPv6 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 167. IPv6 Path MTU Commands

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

IPv6 Neighbor Discovery Prefix Configuration

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

Table 168. IPv6 Neighbor Discovery Prefix Commands

Command Syntax and Usage
`interface ip <125-127>` Enters Interface IP mode. **Command mode**: Global configuration
`ipv6 nd prefix {<IPv6 prefix> <prefix length>} [no-advertise]` Adds a Neighbor Discovery prefix to the interface. The default setting is `enabled`. To disable the prefix and not advertise it in the Prefix Information options in Router Advertisement messages sent from the interface use the `no-advertise` option. Additional prefix options are listed in this table. **Command mode**: Interface IP
`no ipv6 nd prefix [<IPv6 prefix> <prefix length>]|interface|all` Removes the selected Neighbor Discovery prefix(es). If you specify an interface number, all prefixes for the interface are removed. **Command mode**: Interface IP

`ipv6 nd prefix {<IPv6 prefix> <prefix length>}`
`valid-lifetime <0-4294967295> [infinite|variable}`
`prefered-lifetime <0-4294967295> [infinite|variable}`
Configures the Valid Lifetime and (optionally) the Preferred Lifetime of the prefix, in seconds.
The Valid Lifetime is the length of time (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. The default value is 2592000.
The Preferred Lifetime is the length of time (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The default value is 604800.
Note: The Preferred Lifetime value must not exceed the Valid Lifetime value.
Command mode: Interface IP

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

Table 168. IPv6 Neighbor Discovery Prefix Commands (continued)

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

IPv6 Prefix Policy Table Configuration

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

Table 169. IPv6 Prefix Policy Table Options

Command Syntax and Usage
`ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)>` Adds a Prefix Policy Table entry. Enter the following parameters: – IPv6 address prefix – Prefix length – **Precedence**: The precedence is used to sort destination addresses. Prefixes with a higher precedence are sorted before those with a lower precedence. – **Label**: The label allows you to select prefixes based on matching labels. Source prefixes are coupled with destination prefixes if their labels match. **Command mode**: Global configuration
`no ip prefix-policy <IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)>` Removes a prefix policy table entry. **Command mode**: Global configuration
`show ip prefix-policy` Displays the current Prefix Policy Table configuration. **Command mode**: All

Converged Enhanced Ethernet Configuration

Table 170 describes the Converged Enhanced Ethernet (CEE) configuration commands.

Table 170. CEE Commands

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

ETS Global Configuration

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

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

ETS Global Priority Group Configuration

Table 171 describes the global ETS Priority Group configuration options.

Table 171. Global ETS Priority Group Commands

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

Table 171. Global ETS Priority Group Commands

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

Priority Flow Control Configuration

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

Port-level 802.1p PFC Configuration

Table 172 describes the 802.1p Priority Flow Control (PFC) configuration options for the selected port.

Table 172. Port 802.1p PFC Options

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

Table 172. Port 802.1p PFC Options (continued)

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

DCBX Port Configuration

Table 173 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 173. Port DCBX Commands

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

Table 173. Port DCBX Commands (continued)

Command Syntax and Usage
`no cee port <port alias or number> dcbx enable` Disables DCBX on the port. **Command mode**: Global configuration
`cee port <port alias or number> dcbx enable` Enables DCBX on the port. **Command mode**: Global configuration
`show cee port <port alias or number> dcbx` Displays the current port DCBX parameters. **Command mode**: All

Fibre Channel 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 174 describes the FCoE configuration options.

Table 174. FCoE Configuration Commands

Command Syntax and Usage
`fcoe fips enable` Globally turns FIP Snooping on. **Command mode**: Global configuration
`no fcoe fips enable` Globally turns FIP Snooping off. **Command mode**: Global configuration
`[no] fcoe fips timeout-acl` Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system. **Command mode**: Global configuration
`show fcoe information` Displays the current FCoE parameters. **Command mode**: All

FIPS Port Configuration

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

Table 175 describes the port Fibre Channel over Ethernet Initialization Protocol (FIP) Snooping configuration options.

Table 175. Port FIP Snooping Commands

Command Syntax and Usage
`fcoe fips port <`*port alias or number*`> fcf-mode [auto|on|off]` Configures FCoE Forwarding (FCF) on the port, as follows: – `on`: Configures the port as a Fibre Channel Forwarding (FCF) port. – `off`: Configures the port as an FCoE node (ENode). – `auto`: Automatically detect the configuration of the connected device, and configure this port to match. **Command mode**: Global configuration
`fcoe fips port <`*port alias or number*`> enable` Enables FIP Snooping on the port. The default setting is `enabled`. **Note**: If IPv6 ACLs are assigned to the port, you cannot enable FCoE. **Command mode**: Global configuration
`no fcoe fips port <`*port alias or number*`> enable` Disables FIP Snooping on the port. **Command mode**: Global configuration

Virtualization Configuration

Table 176 describes the virtualization configuration options.

Table 176. Virtualization Configurations Options

Command Syntax and Usage
`virt enable` Enables VMready. **Command mode**: Global configuration
`no virt enable` Disables VMready. **Note**: This command deletes all configured VM groups. **Command mode**: Global configuration
`show virt` Displays the current virtualization parameters. **Command mode**: All

VM Policy Bandwidth Management

Table 177 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 177. VM Bandwidth Management Options

Command Syntax and Usage
`virt vmpolicy vmbwidth [`<*MAC address*>`|`<*UUID*>`|`<*name*>`|`<*IP address*>`|`<*index number*>`] txrate` <*64-10000000*> <*max. burst (32-4096)*> <*ACL number*> The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096. The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one. **Command mode**: Global configuration
`[no] virt vmpolicy vmbwidth [`<*MAC address*>`|`<*UUID*>`|`<*name*>`|`<*IP address*>`|`<*index number*>`] bwctrl` Enables or disables bandwidth control on the VM policy. **Command mode**: Global configuration

Table 177. VM Bandwidth Management Options (continued)

Command Syntax and Usage
`no virt vmpolicy vmbwidth [<MAC address>|<UUID>|<name>|<IP address>|<index number>]` Deletes the bandwidth management settings from this VM policy. **Command mode**: Global configuration
`show virt vmpolicy vmbandwidth [<MAC address>|<UUID>|<name>|<IP address>|<index number>]` Displays the current VM bandwidth management parameters. **Command mode**: All

UFP Configuration

Table 178 describes the Unified Fabric Port (UFP) configuration options. UFP allows defining up to 4 virtual ports per physical port. Each virtual port can be set up to operate in a specific mode (access, trunk, tunnel, FCoE) and within predefined bandwidth limits.

Note: vNIC and UFP are mutually exclusive. Only one of them can be globally enabled at any point in time.

Table 178. UFP Commands

Command Syntax and Usage
`[no] ufp enable` Globally enables or disables UFP. **Command mode:** Global configuration
`[no] ufp port <port_no.> enable` Enables or disables UFP on the specified physical ports. **Command mode:** Global configuration
`ufp port <port_no.> vport <1-4>` Enters UFP Virtual Port Configuration mode. **Command mode:** Global configuration
`no ufp port <port_no.> [vport <1-4>]` Disables UFP settings on the specified physical or virtual port. **Command mode:** Global configuration
`[no] enable` Enables or disables the virtual port. **Command mode:** UFP Virtual Port Configuration
`evb profile <1-16>` Applies the specified EVB profile for the port. **Command mode:** UFP Virtual Port Configuration

Table 178. UFP Commands (continued)

Command Syntax and Usage
`network {mode [access|trunk|tunnel|fcoe|auto] | default-vlan <2-4094> | default-tag}` Configures the virtual port network configuration settings: – `mode` configures the virtual port's operating mode: • `access` allows the virtual port to associate only with the default customer VLAN, as defined by the `default-vlan` option. • `trunk` allows the virtual port to associate with up to 256 customer VLANs. • `tunnel` makes the virtual port VLAN agnostic. This is the default setting. • `fcoe` configures the virtual port to carry Fibre Channel over Ethernet traffic when linked to a Fibre Channel virtual Host Bus Adapter. Setting a virtual port in `fcoe` mode enables Priority Flow Control on the physical port. • `auto` integrates UFP with VMReady/802.1qbg. This mode allows dynamic vlan creation for the vport. – `default-vlan` configures the default VLAN ID for the virtual port. – `default-tag` enables tagging egress frames with the default VLAN ID when the virtual port is in access or trunk mode and `default-vlan` is defined. Default setting is disabled. **Note:** VLANs 4002-4005 cannot be used as customer VLANs **Note:** A customer VLAN cannot be configured on multiple virtual ports of the same physical port. **Command mode:** UFP Virtual Port Configuration
`no network default-tag` Disables default VLAN ID tagging on the virtual port. **Command mode:** UFP Virtual Port Configuration
`qos bandwidth {max <10-100>|min <10-100>}` Configures bandwidth allocation for the virtual port: – Configures the minimum bandwidth guaranteed for the virtual port as a percentage of the physical port's bandwidth. The default value is 25. – Configures the maximum bandwidth allowed for this virtual port as a percentage of the physical port's bandwidth. The default value is 100. **Note**: The aggregated minimum bandwidth guaranteed for all the virtual ports within a physical port cannot exceed 100. **Command mode:** UFP Virtual Port Configuration

VM Group Configuration

Table 179 describes the VM group configuration options.A VM group is a collection of members, such as VMs, ports, or trunk groups. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

Table 179. VM Group Commands

Command Syntax and Usage
`virt vmgroup <1-1024> cpu` Enables or disables sending unregistered IPMC to CPU. **Command mode:** Global configuration
`virt vmgroup <1-1024> flood` Enables or disables flooding unregistered IPMC. **Command mode:** Global configuration
`virt vmgroup <1-1024> optflood` Enables or disables optimized flooding. **Command mode:** Global configuration
`virt vmgroup <1-1024> vlan <VLAN number>` Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group. **Note**: If you add a VM profile to this group, the group will use the VLAN assigned to the profile. **Command mode:** Global configuration
`[no] virt vmgroup <1-1024> vmap <VMAP number> intports|extports` Assigns the selected VLAN Map to this group. You can choose to limit operation of the VLAN Map to internal ports only or external ports only. If you do not select a port type, the VMAP is applied to the entire VM Group. For more information about configuring VLAN Maps, see "VMAP Configuration" on page 181. **Command mode:** Global configuration
`[no] virt vmgroup <1-1024> tag` Enables or disables VLAN tagging on ports in this VM group. **Command mode:** Global configuration
`virt vmgroup <1-1024> vm [<MAC address>|<UUID>|<name>|<IP address>| <index number>]` Adds a VM to the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (`virt vmware vcspec`). The VM index number is found in the VM information dump (`show virt vm`). **Note**: If the VM is connected to a port that is contained within the VM group, do not add the VM to the VM group. **Command mode:** Global configuration

Table 179. VM Group Commands (continued)

Command Syntax and Usage
`no virt vmgroup <1-1024> vm [<MAC address>|<UUID>|<name>|<IP address>|<index number>]` Removes a VM from the VM group. Enter a unique identifier to select a VM. The UUID and name parameters apply only if Virtual Center information is configured (`virt vmware vcspec`). The VM index number is found in the VM information dump (`show virt vm`). **Command mode:** Global configuration
`virt vmgroup <1-1024> profile <profile name (1-39 characters)>` Adds the selected VM profile to the VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024> profile` Removes the VM profile assigned to the VM group. **Note:** This command can only be used if the VM group is empty (only has the profile assigned). **Command mode:** Global configuration
`virt vmgroup <1-1024> port <port number or alias>` Adds the selected port to the VM group. **Note**: A port can be added to a VM group only if no VMs on that port are members of the VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024> port <port number or alias>` Removes the selected port from the VM group. **Command mode:** Global configuration
`virt vmgroup <1-4096> vport <port alias or number>` Adds the selected virtual port to the VM group. **Command mode:** Global configuration
`no virt vmgroup <1-4096> vport <port alias or number>` Removes the selected virtual port from the VM group. **Command mode:** Global configuration
`virt vmgroup <1-1024> portchannel <trunk number>` Adds the selected trunk group to the VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024> portchannel <trunk number>` Removes the selected trunk group from the VM group. **Command mode:** Global configuration

Table 179. VM Group Commands (continued)

Command Syntax and Usage
`virt vmgroup <1-1024> key <1-65535>` Adds an LACP *admin key* to the VM group. LACP trunks formed with this *admin key* will be included in the VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024> key <1-65535>` Removes an LACP *admin key* from the VM group. **Command mode:** Global configuration
`virt vmgroup <1-1024> validate [basic|advanced]` Enables MAC address spoof prevention for the specified VM group. Default setting is disabled. – `basic` validation ensures lightweight port-based protection by cross-checking the VM MAC address, switch port and switch ID between the switch and the hypervisor. Applicable for “trusted” hypervisors, which are not susceptible to duplicating or reusing MAC addresses on virtual machines. – `advanced` validation ensures heavyweight VM-based protection by cross-checking the VM MAC address, VM UUID, switch port and switch ID between the switch and the hypervisor. Applicable for “untrusted” hypervisors, which are susceptible to duplicating or reusing MAC addresses on virtual machines. **Command mode:** Global configuration
`no virt vmgroup <1-1024> validate` Disables MAC address spoof prevention for the specified VM group. **Command mode:** Global configuration
`no virt vmgroup <1-1024>` Deletes the VM group. **Command mode:** Global configuration
`show virt vmgroup <1-1024>` Displays the current VM group parameters. **Command mode:** All

VM Check Configuration

Table 180 describes the VM Check validation options used for MAC address spoof prevention.

Table 180. VM Check Configuration Options

Command Syntax and Usage
`virt vmcheck acls max` <*1-640*> Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50. **Command mode:** Global configuration
`no virt vmcheck acls` Disables ACL-based MAC address spoofing prevention in advanced validation mode. **Command mode:** Global configuration
`virt vmcheck action basic {link|log}` Sets up action taken when detecting MAC address spoofing in basic validation mode: – `link` registers a syslog entry and disables the corresponding switch port – `log` registers a syslog entry Default setting is `link`. **Command mode:** Global configuration
`virt vmcheck action advanced {acl|link|log}` Sets up action taken when detecting MAC address spoofing in advanced validation mode: – `acl` registers a syslog entry and installs an ACL to drop traffic incoming on the corresponding switch port originating from the spoofed MAC address – `link` registers a syslog entry and disables the corresponding switch port – `log` registers a syslog entry Default setting is `acl`. **Command mode:** Global configuration
`[no] virt vmcheck trust` <*ports*> Enables or disables trusted ports for VM communication. By default, all ports are disabled. **Command mode:** Global configuration
`show virt vmcheck` Displays the current VM Check settings. See page 51 for sample output. **Command mode:** Global configuration

VM Profile Configuration

Table 181 describes the VM Profiles configuration options.

Table 181. VM Profiles Commands

Command Syntax and Usage
`virt vmprofile <profile name (1-39 characters)>` Defines a name for the VM profile. **Command mode:** Global configuration
`no virt vmprofile <profile name (1-39 characters)>` Deletes the selected VM profile. **Command mode:** Global configuration
`virt vmprofile edit <profile name (1-39 characters)> vlan <VLAN number>` Assigns a VLAN to the VM profile. **Command mode:** Global configuration
`[no] virt vmprofile edit <profile name (1-39 characters)> shaping [<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>]` Configures traffic shaping parameters implemented in the hypervisor, as follows: – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters. **Command mode:** Global configuration
`[no] virt vmprofile edit <profile name (1-39 characters)> eshaping [<average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>]` Configures traffic egress shaping parameters implemented in the hypervisor, as follows: – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters. **Command mode:** Global configuration
`show virt vmprofile [<profile name>]` Displays the current VM Profile parameters. **Command mode:** All

VMWare Configuration

Table 182 describes the VMware configuration options.When the user configures the VMware Virtual Center, the VM Agent module in the switch can perform advanced functionality by communicating with the VMware management console. The Virtual Center provides VM and Host names, IP addresses, Virtual Switch and port group information. The VM Agent on the switch communicates with the Virtual Center to synchronize VM profiles between the switch and the VMware virtual switch.

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

Table 182. VM Ware Commands

Command Syntax and Usage
`virt vmware hbport <1-65535>` Configures the UDP port number used for heartbeat communication from the VM host to the Virtual Center. The default value is port 902. **Command mode:** Global configuration
`[no] virt vmware vcspec [<IP address>|[<username> noauth]` Defines the Virtual Center credentials on the switch. Once you configure the Virtual Center, VM Agent functionality is enabled across the system. You are prompted for the following information: – IP address of the Virtual Center – User name and password for the Virtual Center – Whether to authenticate the SSL security certificate (yes or no) **Command mode:** Global configuration
`virt vmware hello [enable|haddr <IP_address>|hport <port_no>|htimer <1-60>]` Configures CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors facilitates MAC address spoof prevention. Default setting is disabled. – `enable` enables CDP advertisements transmission. – `haddr` advertises a specific IP address instead of the default management IP. – `hport` enables ports on which CDP advertisements are sent. – `htimer` sets the number of seconds between successive CDP advertisements. Default value is 30. **Command mode:** Global configuration
`no virt vmware hello [enable|hport <port_no>]` Disables CDP advertisement transmissions completely or only on specific ports. **Command mode**: Global configuration
`show virt vmware` Displays the current VMware parameters. **Command mode:** All

Miscellaneous VMready Configuration

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the IBM Networking OS CLI, ISCLI and the Miscellaneous VMready Configuration Menu. Table 182 describes the VMready configuration options.

Table 183. VMware Miscellaneous Options

Command Syntax and Usage
`virt vmrmisc oui` *< 3 byte VM MAC OUI> <Vendor Name>* Adds a MAC OUI. **Command mode**: Global configuration
`no virt vmrmisc oui` *< 3 byte VM MAC OUI>* Removes a MAC OUI. **Command mode**: Global configuration
`show virt oui` Displays all the configured MAC OUIs. **Command mode**: All
`virt vmrmisc lmac` Enables the switch to treat locally administered MAC addresses as VMs. **Command mode**: Global configuration
`no virt vmrmisc lmac` Disables the switch from treating locally administered MAC addresses as VMs. **Command mode**: Global configuration

Edge Virtual Bridge Configuration

You can configure your switch to use Edge Virtual Bridging (EVB). Table 184 describes the EVB configuration options.

Table 184. Edge Virtual Bridge Configuration Options

Command Syntax and Usage
`virt evb vsidb <VSIDB_number>` Enter Virtual Station Interface Database configuration mode. **Command mode:** Global configuration
`clear virt evb vsidb [mgrid <0-255> | typeid <1-16777215> | version <0-255>]` Clears local VSI types cache. **Command mode**: All
`clear virt evb vsi [mac-address | port <port alias or number> | type-id <1-16777215> | vlan <1-4094>]` Clears VSI database associations. **Command mode**: All
`host <IP address> [mgt-port|extm-port]` Sets the Virtual Station Interface Type database manager IPv4/IPv6 address and the port used for the connection. By default, the management port is used. **Command mode:** VSI Database
`port <1-65534>` Sets the Virtual Station Interface Type database manager port. **Command mode:** VSI Database
`filename <File name>` Sets the Virtual Station Interface Type database document name. **Command mode:** VSI Database
`filepath <File path>` Sets the Virtual Station Interface Type database document path. **Command mode:** VSI Database
`protocol {http | https}` Sets the Virtual Station Interface Type database transport protocol. The default setting is HTTP. **Command mode:** VSI Database
`update-interval <5-300>` Sets the Virtual Station Interface Type database update interval in seconds. A value of “0” disables periodic updates. **Command mode:** VSI Database

Table 184. Edge Virtual Bridge Configuration Options

Command Syntax and Usage
`show virt evb vsitypes [mgrid <0-255> | typeid <1-16777215> | version <0-255>` Displays the current Virtual Station Interface Type database parameters. **Command mode:** All
`show virt evb vsidb <VSIDB_number>` Displays the current Virtual Station Interface database information. **Command mode:** All
`no virt evb vsidb <VSIDB_number>` Resets the Virtual Station Interface Type database information to the default values. **Command mode:** Global configuration

Edge Virtual Bridge Profile Configuration

Table 185 describes the Edge Virtual Bridge profile configuration options.

Table 185. Edge Virtual Bridge VSI Type Profile Configuration Options

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

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 186. 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: – `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 186. SPAR Configuration Options (continued)

Command Syntax and Usage
`domain local <1-256> {enable|member <port no.>|name <text>|vlan <2-4094>}` Configures the SPAR's local domains: – `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. **Command mode:** SPAR Configuration
`no domain local <1-256> [enable|member <port no.> |vlan]` Deletes the SPAR local VLAN domains: – `enable` disables the SPAR local domains – `member` deletes SPAR local domains server ports – `vlan` deletes SPAR local domains vlan. **Command mode:** SPAR Configuration
`domain mode {passthrough|local}` Configures the SPAR domain mode: – `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 **Command mode:** SPAR Configuration
`show spar <1-8> [domain [default|local <1-256>] |uplink]` Displays the SPAR settings: – `domain` filters only the SPAR domain related settings • `default` filters only SPAR default domain settings • `local <1-256>` filters only SPAR local domains settings – `uplink` filters only SPAR uplink settings **Command mode:** All

Service Location Protocol Configuration

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

- User Agents (UA) are devices requesting services.
- Service Agents (SA) are devices providing services.

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

When SLP is enabled, the SI4093 10Gb System Interconnect Module (SIM) behaves as a Service Agent providing systems management services.

Table 187. Service Location Protocol

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

Configuration Dump

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

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

The configuration is displayed with parameters that have been changed from the default values. The screen display can be captured, edited, and placed in a script file, which can be used to configure other switches through a Telnet connection. When using Telnet to configure a new switch, paste the configuration commands from the script file at the command line prompt of the switch. The active configuration can also be saved or loaded via FTP/TFTP, as described on page 252.

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 188. General Operations Commands

Command Syntax and Usage
`password` *<1-128 characters>* Allows the user to change the password. You must enter the current password in use for validation. The switch prompts for a new password between 1-128 characters. **Command Mode**: Privileged EXEC
`clear logging` Clears all Syslog messages. **Command Mode**: Privileged EXEC
`ntp send` Allows the user to send requests to the NTP server. **Command Mode**: Privileged EXEC

Operations-Level Port Commands

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

Table 189. Port Operations Commands

Command Syntax and Usage
`no interface port <`*port number or alias*`> shutdown` Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`interface port <`*port number or alias*`> shutdown` Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`[no] interface portchannel <`*1-52*`> shutdown` Temporarily enables or disables the specified port channel. The port channel will be returned to its configured operation mode when the switch is reset. **Command Mode**: Privileged EXEC
`[no] interface portchannel lacp <`*1-65535*`> shutdown` Temporarily enables or disables specified LACP trunk groups. **Command Mode**: Privileged EXEC
`show interface port <`*port number or alias*`> operation` Displays the port interface operational state. **Command Mode**: Privileged EXEC

Operations-Level FCoE Commands

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

Table 190. FCoE Operations Commands

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

Protected Mode Options

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

Table 191. Protected Mode Options

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

Table 191. Protected Mode Options (continued)

Command Syntax and Usage
`no protected-mode enable` Turns Protected Mode `off`. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options. **Command Mode**: Global Configuration
`show protected-mode` Displays the current Protected Mode configuration. **Command Mode**: Global Configuration

Feature on Demand Key Options

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

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

Table 192. Feature on Demand Key Options

Command Syntax and Usage
`software-key` Enter FOD Key mode. **Command mode:** Privileged EXEC

`enakey address` <*hostname or IP address*> `keyfile` <*file name*> `protocol tftp|sftp mgt`
Unlocks the software port expansion feature. You are prompted to enter the host name or IP address of the server where the license key is stored, and the license key file name, as follows:
– `46Port`
– `64Port`
Note: You must upgrade to `46Port` port mode before you can upgrade to `64Port` port mode.
Command mode: FOD Key mode
Use the following command to perform the same action, regardless the command mode:
`copy tftp software-key address` <*hostname or IP address*> `keyfile` <*file name*> `mgt`

`ptkey address` <*hostname or IP address*> `key` <*feature name*> `protocol tftp|sftp file` <*file name*> `mgt`
Loads the specified key file to a server.
Command mode: FOD Key mode
Use the following command to perform the same action, regardless the command mode:
`copy software-key address` <*hostname or IP address*> `key` <*file name*> `protocol tftp|sftp file` <*file name*> `mgt`

`invkeys address` <*hostname or IP address*> `invfile` <*file name*> `protocol tftp|sftp mgt`
Loads key code inventory information to a server.
Command mode: FOD Key mode
Use the following command to perform the same action, regardless the command mode:
`copy invkeys address` <*hostname or IP address*> `invfile` <*file name*> `protocol tftp|sftp mgt`

Table 192. Feature on Demand Key Options

Command Syntax and Usage
`rmkey key <`*feature name*`>` Removes the specified software feature. **Command mode:** FOD Key mode
`show software-key` Removes the specified software feature. **Command mode:** All
`exit` Exit from Feature on Demand Key mode. **Command mode:** FOD Key mode

Chapter 6. Boot Options

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

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

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

The boot options are discussed in the following sections.

Scheduled Reboot

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

Table 193. Boot Scheduling Options

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

Netboot Configuration

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

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

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

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

Table 194. Netboot Options (/boot/netboot)

Command Syntax and Usage
`boot netboot enable` Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file. **Command mode:** Global configuration
`no boot netboot enable` Disables Netboot. **Command mode:** Global configuration
`[no] boot netboot tftp <`*IP address*`>` Configures the IP address of the TFTP server used for manual configuration. This server is used if DHCP is not enabled, or if the DHCP server does not return the required information. **Command mode:** Global configuration

`[no] boot netboot cfgfile <`*1-31 characters*`>`
Defines the file path for the configuration file on the TFTP server. For example:
`/directory/sub/config.cfg`
Command mode: Global configuration

`show boot` Displays the current Netboot parameters. **Command mode:** All

Flexible Port Mapping

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

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

Table 195 lists the Flexible Port Mapping command options.

Table 195. Flexible Port Mapping Options

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

The switch must be reset for port mapping changes to take effect.

QSFP Port Configuration

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

Table 196. Netboot Options (/boot/qsfp-40Gports)

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

Updating the Switch Software Image

The switch software image is the executable code running on the SI4093 10Gb System Interconnect Module (SIM). 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 (SIM), 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 (SIM) 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 (SIM) 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 (SIM) 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 197. General Maintenance Commands

Command Syntax and Usage
`show flash-dump-uuencode` Displays dump information in uuencoded format. For details, see page 282. **Command mode:** All
`copy flash-dump tftp` Saves the system dump information via TFTP. For details, see page 283. **Command mode:** All except User EXEC
`copy flash-dump ftp` Saves the system dump information via FTP. For details, see page 283. **Command mode:** All except User EXEC
`clear flash-dump` Clears dump information from flash memory. **Command mode:** All except User EXEC
`show tech-support [l2|l3|link|port]` Dumps all SI4093 information, statistics, and configuration. You can log the output (`tsdmp`) into a file. To filter the information, use the following options: – `l2` displays only Layer 2-related information – `l3` displays only Layer 3-related information – `link` displays only link status-related information – `port` displays only port-related information **Command mode:** All except User EXEC

Table 197. General Maintenance Commands

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

Forwarding Database Maintenance

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

Table 198. FDB Manipulation Commands

Command Syntax and Usage
`show mac-address-table address` <*MAC address*> Displays a single database entry by its MAC address. If not specified, you are prompted for the MAC address of the device. Enter the MAC address using one of the following formats: – `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) – `xxxxxxxxxxxx` (such as `080020123456`) **Command mode:** All except User EXEC
`show mac-address-table interface port` <*port number or alias*> Displays all FDB entries for a particular port. **Command mode:** All except User EXEC
`show mac-address-table portchannel` <*trunk group number*> Displays all FDB entries for a particular trunk group. **Command mode:** All
`show mac-address-table private-vlan` <*VLAN number*> Displays all FDB entries on a single private VLAN. **Command mode:** All
`show mac-address-table vlan` <*VLAN number*> Displays all FDB entries on a single VLAN. **Command mode:** All except User EXEC
`show mac-address-table state {forward|trunk|unknown}` Displays all FDB entries of a particular state. **Command mode:** All except User EXEC
`show mac-address-table static` Displays static entries in the FBD. **Command mode:** All except User EXEC
`no mac-address-table static {`<*MAC address*>`|all}` Removes static FDB entries. **Command mode:** All except User EXEC
`clear mac-address-table static` Clears all static entries from the Forwarding Database. **Command mode:** All except User EXEC

Table 198. FDB Manipulation Commands (continued)

Command Syntax and Usage
`clear mac-address-table` Clears the entire Forwarding Database from switch memory. **Command mode:** All except User EXEC

Debugging Commands

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

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

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

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

Table 199. Miscellaneous Debug Commands

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

`debug mp-trace`
Displays the Management Processor trace buffer. Header information similar to the following is shown:
`MP trace buffer at 13:28:15 Fri May 25, 2001; mask: 0x2ffdf748`
The buffer information is displayed after the header.
Command mode: All except User EXEC

`debug dumpbt` Displays the backtrace log. **Command mode:** All except User EXEC
`debug mp-snap` Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred. **Command mode:** All except User EXEC
`clear flash-config` Deletes all flash configuration blocks. **Command mode:** All except User EXEC

Table 199. Miscellaneous Debug Commands

Command Syntax and Usage
`[no] debug lacp packet [receive|transmit|both] [port <`*port numbers*`>]` Enables/disables debugging for Link Aggregation Control Protocol (LACP) packets on all ports running LACP. The following parameters are available: – `receive` filters only LACP packets received – `transmit` filters only LACP packets sent – `both` filters LACP packets either sent or received – `port` filters LACP packets sent/received on specific ports By default, LACP debugging is disabled. **Command mode:** Privileged EXEC

LLDP Cache Manipulation

Table 200 describes the LLDP cache manipulation commands.

Table 200. LLDP Cache Manipulation commands

Command Syntax and Usage
`show lldp port` *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information. **Command mode:** All
`show lldp receive` Displays information about the LLDP receive state machine. **Command mode:** All
`show lldp transmit` Displays information about the LLDP transmit state machine. **Command mode:** All
`show lldp remote-device [`*<1-256>*`|detail]` Displays information received from LLDP -capable devices. For more information, see page 32. **Command mode:** All
`show lldp` Displays all LLDP information. **Command mode:** All
`clear lldp` Clears the LLDP cache. **Command mode:** All

Uuencode Flash Dump

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

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

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

Note: Dump information is not cleared automatically. In order for any subsequent dump information to be written to flash memory, you must manually clear the dump region. For more information on clearing the dump region, see page 284.

To access dump information, enter:

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

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

```
No FLASH dump available.
```

TFTP or FTP System Dump Put

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

Note: If the TFTP/FTP server is running SunOS or the Solaris operating system, the specified `copy flash-dump tftp` (or `ftp`) file must exist *prior* to executing the `copy flash-dump tftp` command (or `copy flash-dump tftp`), and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current dump data.

To save dump information via TFTP, enter:

```
Router# copy flash-dump tftp  <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 (SIM) (SI4093) uses the following syntax when outputting system log (syslog) messages:

<*Time stamp*> <*IP/Hostname*><*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

- <*IP/Hostname*>

  The hostname is displayed when configured.

  For example: 1.1.1.1

- <*Log Label*>

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

- <*Thread ID*>

  This is the software thread that reports the log message. For example: stg, ip, console, telnet, vrrp, system, web server, ssh, bgp

- <*Message*>: The log message

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

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

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
BGP	session with <*IP address*> failed (bad event:<*event*>)
BGP	session with <*IP address*> failed <*reason*> Reasons: • Connect Retry Expire • Holdtime Expire • Invalid • Keepalive Expire • Receive KEEPALIVE • Receive NOTIFICATION • Receive OPEN • Receive UPDATE • Start • Stop • Transport Conn Closed • Transport Conn Failed • Transport Conn Open • Transport Fatal Error
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
IP	Route table full
MGMT	Maximum number of login failures (<*threshold*>) has been exceeded.
OSPF	Interface IP <*IP address*>, Interface State {Down | Loopback | Waiting | P To P | DR | BackupDR | DR Other}: Interface down detached
OSPF	LS Database full: likely incorrect/missing routes or failed neighbors
OSPF	Neighbor Router ID <*router ID*>, Neighbor State {Down | Attempt | Init | 2 Way | ExStart | Exchange | Loading | Full | Loopback | Waiting | P To P | DR | BackupDR | DR Other}
OSPF	OSPF Route table full: likely incorrect/missing routes
STP	CIST new root bridge
STP	CIST topology change detected
STP	own BPDU received from port <*port*>
STP	Port <*port*>, putting port into blocking state
STP	STG <*STG*>, new root bridge
STP	STG <*STG*>, topology change detected
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <key>
VRRP	Received <x> virtual routers instead of <y>

Thread	LOG_ALERT Message (continued)
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 <*username*>.
	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	/* Config changes at <time> by <*username*> */ <*config diff*> /* Done */
MGMT	<*username*> ejected from BBI
MGMT	<*username*>(<*user type*>) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	<*username*>(<*user type*>) login {on Console | from host <*IP address*>}
MGMT	boot kernel download completed. Now writing to flash.
MGMT	boot kernel downloaded {from host <*hostname*> | via browser}, filename too long to be displayed, software version <*version*>
MGMT	boot kernel downloaded from host <*hostname*>, file'<*filename*>', software version <*version*>
MGMT	Can't downgrade to image with only single flash support
MGMT	Could not revert unsaved changes
MGMT	Download already currently in progress. Try again later via {Browser | BBI}
MGMT	Error in setting the new config
MGMT	Failed to allocate buffer for diff track.
MGMT	Firmware download failed to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}
MGMT	Firmware downloaded to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Flash dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting

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]
MGMT	new configuration saved from {BBI | ISCLI | SNMP}
MGMT	scp*<username>*(*<user type>*) {logout | ejected | idle timeout | connection closed} from {Console | Telnet/SSH}
MGMT	scp*<username>*(*<user type>*) login {on Console | from host *<IP address>*}
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host *<hostname>* | via browser}, filename too long to be displayed, software version *<version>*
MGMT	SP boot kernel downloaded from host *<hostname>*, file '*<filename>*', software version *<version>*
MGMT	Starting Firmware download for {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to *<hostname>*:*<filename>*
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.

Thread	LOG_INFO Message (continued)
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: • Boot watchdog reset • console PANIC command • console RESET KEY • hard reset by SNMP • hard reset by WEB-UI • hard reset from console • hard reset from Telnet • low memory • MM Cycled Power Domain • power cycle • Reset Button was pushed • reset by SNMP • reset by WEB-UI • reset from console • reset from EM • reset from Telnet/SSH • scheduled reboot • SMS-64 found an over-voltage • SMS-64 found an under-voltage • software ASSERT • software PANIC • software VERIFY • Telnet PANIC command • unknown reason • watchdog timer

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 <*interface*>.
CFG	Multicast should be disabled to run RIPv2 in RIPv1 compatibility mode on interface <*interface*>.
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
MGMT	The software demo license for Upgrade2 will expire in 10 days. The switch will automatically reset to the factory configuration after the license expires. Please backup your configuration or enter a valid license key so the configuration will not be lost.
NTP	cannot contact [primary | secondary] NTP server <*IP address*>
SYSTEM	I2C device <*ID*> <*description*> set to access state <*state*> [from CLI]
TEAMING	error, action is undefined
TEAMING	is down, but teardown is blocked
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

A

B

C

D

E

F

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 00CG965

Printed in USA

(IP) P/N: 00CG965