IBM Networking OS 7.5

Menu-Based CLI Command Reference

for the CN4093 10Gb Converged Scalable Switch

IBM Networking OS 7.5

Menu-Based CLI Command Reference

for the CN4093 10Gb Converged Scalable Switch

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 (November 2012)

Contents

Preface

This *Menu-Based CLI Command Reference* describes how to configure and use the IBM Networking OS 7.5 software with your IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch (CN4093).

For documentation on installing the switches physically, see the *Installation Guide* for your CN4093. For details about configuration and operation of your CN4093, see the *IBM Networking OS 7.5 Application Guide*.

Who Should Use This Book

This book is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, the IEEE 802.1D Spanning Tree Protocol, and SNMP configuration parameters.

How This Book Is Organized

Chapter 1, "The Command Line Interface," describes how to connect to the switch and access the information and configuration menus.

Chapter 2, "First-Time Configuration," describes how to use the Setup utility for initial switch configuration and how to change the system passwords.

Chapter 2, "Menu Basics," provides an overview of the menu system, including a menu map, global commands, and menu shortcuts.

Chapter 3, "The Information Menu," shows how to view switch configuration parameters.

Chapter 4, "The Statistics Menu," shows how to view switch performance statistics.

Chapter 5, "The Configuration Menu," shows how to configure switch system parameters, ports, VLANs, Spanning Tree Protocol, SNMP, Port Mirroring, IP Routing, Port Trunking, and more.

Chapter 6, "The Operations Menu," shows how to use commands which affect switch performance immediately, but do not alter permanent switch configurations (such as temporarily disabling ports). The menu describes how to activate or deactivate optional software features.

Chapter 7, "The Boot Options Menu," 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 8, "The Maintenance Menu," 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, "System Log Messages," shows a listing of syslog messages.

Appendix B, "SNMP Agent," lists the Management Interface Bases (MIBs) supported in the switch software.

"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: **`/info/sys/gen`**
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 **`/cfg/l2/vlan/vmap {add|rem}`** *<1-127>* you enter: **`/cfg/l2/vlan/vmap add 1`** or **`/cfg/l2/vlan/vmap rem 1`**

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 **`/cfg/sys/dhcp [mgta|mgtb] enable`** you enter **`/cfg/sys/dhcp mgta enable`** or **`/cfg/sys/dhcp mgtb enable`**
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 **`/cfg/l3/route/ecmphash [sip|dipsip]`** you enter: **`/cfg/l3/route/ecmphash sip`** or **`/cfg/l3/route/ecmphash dipsip`**

How To Get Help

If you need help, service, or technical assistance, visit our website at the following address:

You also can visit our web site at the following address:

`http://www.ibm.com/support`

Click the **Support** tab.

The warranty card received with your product provides details for contacting a customer support representative. If you are unable to locate this information, please contact your reseller. Before you call, prepare the following information:

- Serial number of the switch unit
- Software release version number
- Brief description of the problem and the steps you have already taken
- Technical support dump information (`# show tech-support`)

Chapter 1. The Command Line Interface

Your CN4093 10Gb Converged Scalable Switch (CN4093) is ready to perform basic switching functions right out of the box. Some of the more advanced features, however, require some administrative configuration before they can be used effectively.

The extensive IBM Networking OS switching software included in your switch provides a variety of options for accessing and configuring the switch:

- A built-in, text-based command line interface and menu system for access via a Telnet session or serial-port connection
- SNMP support for access through network management software such as IBM Director or HP OpenView
- IBM Networking OS Browser-Based Interface (BBI)

The command line interface is the most direct method for collecting switch information and performing switch configuration. Using a basic terminal, you are presented with a hierarchy of menus that enable you to view information and statistics about the switch, and to perform any necessary configuration.

This chapter explains how to access the Command Line Interface (CLI) for the switch.

Connecting to the Switch

You can access the command line interface in any one of the following ways:

- Using a Telnet connection via the chassis management module
- Using a Telnet connection over the network
- Using a SSH connection via the management module
- Using a serial connection via the serial port on the CN4093

Accessing the Switch

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the CN4093. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as follows:

- User interaction with the switch is completely passive—nothing can be changed on the CN4093. Users may display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operators can only effect temporary changes on the CN4093. These changes will be 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.
- Administrators are the only ones that may make permanent changes to the switch configuration—changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the CN4093. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique surnames and passwords. Once you are connected to the switch via local Telnet, remote Telnet, or SSH, you are prompted to enter a password. The default user names/password for each access level are listed in the following table.

Note: It is recommended that you change default switch passwords after initial configuration and as regularly as required under your network security policies. For more information, see “Setting Passwords” on page 11.

Table 2. 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 manages all functions of the switch. The Operator can reset ports, except the management ports.	`oper`
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the CN4093, including the ability to change both the user and administrator passwords.	`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.

Setup vs. CLI

Once the administrator password is verified, you are given complete access to the switch. If the switch is still set to its factory default configuration, the system will ask whether you wish to run Setup, a utility designed to help you through the first-time configuration process. If the switch has already been configured, the Main Menu of the CLI is displayed instead.

The following table shows the Main Menu with administrator privileges.

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

Note: If you are accessing a user account, some menu options are not available.

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see “Menu Basics” on page 9.”

Idle Timeout

By default, the switch will disconnect your Telnet session after 10 minutes of inactivity. This function is controlled by the idle timeout parameter, which can be set from 1 to 60 minutes, or disabled when set to 0. For information on changing this parameter, see “System Configuration Menu” on page 196.

Chapter 2. Menu Basics

The IBM Networking OS Command Line Interface (CLI) is used for viewing switch information and statistics. In addition, the administrator can use the CLI for performing all levels of switch configuration.

To make the CLI easy to use, the various commands have been logically grouped into a series of menus and sub-menus. Each menu displays a list of commands and/or sub-menus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main Menu commands, and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

The Main Menu

The Main Menu appears after a successful connection and login. The following table shows the Main Menu for the administrator login. Some features are not available under the user login.

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

Menu Summary

The following menus are available from the Main Menu:

- **Information Menu**

  Provides sub-menus for displaying information about the current status of the switch: from basic system settings to VLANs, and more.

- **Statistics Menu**

  Provides sub-menus for displaying switch performance statistics. Included are port, IF, IP, ICMP, TCP, UDP, SNMP, routing, ARP, DNS, and VRRP statistics.

- **Configuration Menu**

  This menu is available only from an administrator login. It includes sub-menus for configuring every aspect of the switch. Changes to configuration are not active until explicitly applied. Changes can be saved to non-volatile memory.

- **Operations Menu**

  Operations-level commands are used for making immediate and temporary changes to switch configuration. This menu is used for bringing ports temporarily in and out of service, enabling or disabling FDB learning on a port, or sending NTP requests. It is also used for activating or deactivating optional software packages.

- **Boot Options Menu**

  This menu is used for upgrading switch software, selecting configuration blocks, and for resetting the switch when necessary.

- **Maintenance Menu**

  This menu is used for debugging purposes, enabling you to generate a dump of the critical state information in the switch, and to clear entries in the forwarding database and the ARP and routing tables.

Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes.

For help on a specific command, type `help`. You will see the following screen:

```
Global Commands: [can be issued from any menu]
help              list              up                print
pwd               lines             verbose           exit
quit              config            diff              apply
save              revert            ping              traceroute
telnet            history           pushd             popd
who               chpass_p          chpass_s          clock
mv                dir

The following are used to navigate the menu structure:
    .  Print current menu
   ..  Move up one menu level
    /  Top menu if first, or command separator
    !  Execute command from history
```

Table 3. Description of Global Commands

Command	Action
`?` *command* **or** `help`	Provides more information about a specific command on the current menu. When used without the *command* parameter, a summary of the global commands is displayed.
`.` or `print`	Display the current menu.
`list`	Lists the commands available at the current level. You may follow the list command with a text string, and list all of the available commands that match the string.
`..` or `up`	Go up one level in the menu structure.
`/`	If placed at the beginning of a command, go to the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.

Table 3. Description of Global Commands (continued)

Command	Action
`lines [<n>]`	Set the number of lines (*n*) that display on the screen at one time. The default is 28 lines. When used without a value, the current setting is displayed. Set lines to a value of 0 (zero) to disable pagination.
`diff`	Show any pending configuration changes.
`apply`	Apply pending configuration changes.
`save`	Write configuration changes to non-volatile flash memory.
`revert`	Remove pending configuration changes between "`apply`" commands. Use this command to remove any configuration changes made since last `apply`.
`revert apply`	Remove pending or applied configuration changes between "`save`" commands. Use this command to remove any configuration changes made since last `save`.
`exit` or `quit`	Exit from the command line interface and log out.
`config`	Displays the switch configuration dump.
`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`). The DNS parameters must be configured if specifying hostnames (see "Domain Name System Configuration Menu" on page 369).

Table 3. Description of Global Commands (continued)

Command	Action
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: `traceroute` *<hostname>*|*<IP address>* [*<max-hops (1-32)>* [*<msec-delay (1-4294967295)>*]] Where *hostname/IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-32 devices), and *msec-delay* (optional) is the number of milliseconds to wait for the response. As with `ping`, the DNS parameters must be configured if specifying hostnames.
`pwd`	Display the command path used to reach the current menu.
`verbose` *n*	Sets the level of information displayed on the screen: `0` = Quiet: Nothing appears except errors—not even prompts. `1` = Normal: Prompts and requested output are shown, but no menus. `2` = Verbose: Everything is shown. When used without a value, the current setting is displayed.
`telnet`	This command is used to telnet out of the switch. The format is as follows: `telnet` *<hostname>*|*<IP address>* [*<port>*] Where *IP address* is the hostname or IP address of the device.
`history`	This command displays the most recent commands.
`pushd`	Save the current menu path, so you can jump back to it using `popd`.
`popd`	Go to the menu path and position previously saved by using `pushd`.
`who`	Displays a list of users that are logged on to the switch.
`chpass_p`	Configures the password for the primary TACACS+ server.
`chpass_s`	Configures the password for the secondary TACACS+ server.
`clock`	Displays the configured date and time for the switch.
`mv` ***file1 file2***	Move (rename) a file
`dir`	Lists image and configuration files. The format is as follows: `dir [images|configs]`

Command Line History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

Table 4. Command Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 64 previously entered commands.
`!!`	Repeat the last entered command.
`!`*n*	Repeat the n^{th} command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the *previou*s command from the history list. This can be used multiple times to work backward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the *next* command from the history list. This can be used multiple times to work forward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the *end* of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor *back* one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor *forward* one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	*Delete* one character at the cursor position.
<Ctrl-k>	*Kill* (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command Line Interface Shortcuts

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

CLI List and Range Inputs

For CLI 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 `/info/vlan` command permits the following options:

```
# /info/l2/vlan                        (show all VLANs)
# /info/l2/vlan 1                      (show only VLAN 1)
# /info/l2/vlan 1,3,4095               (show listed VLANs)
# /info/l2/vlan 1-20                   (show range 1 through 20)
# /info/l2/vlan 1-5,90-99,4090-4095    (show multiple ranges)
# /info/l2/vlan 1-5,19,20,4090-4095    (show 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 enable multiple ports with one command:

```
# /cfg/port 1-4/ena                    (Enable ports 1 though 4)
```

Note: Port ranges accept only port numbers, not aliases such as INT1 or EXT1.

Command Stacking

As a shortcut, you can type multiple commands on a single line, separated by forward slashes (/). You can connect as many commands as required to access the menu option that you want. For example, the keyboard shortcut to access the Spanning Tree Port Configuration Menu from the `Main#` prompt is as follows:

```
Main# cfg/l2/stg 1/port
```

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same menu or sub-menu. For example, the command shown above could also be entered as follows:

```
Main# c/l2/stg 1/po
```

Tab Completion

By entering the first letter of a command at any menu prompt and hitting <Tab>, the CLI will display all commands or options in that menu that begin with that letter. Entering additional letters will further refine the list of commands or options displayed. If only one command fits the input text when <Tab> is pressed, that command will be supplied on the command line, waiting to be entered. If the <Tab> key is pressed without any input on the command line, the currently active menu will be displayed.

Chapter 3. The Information Menu

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.

/info
Information Menu

```
[Information Menu]
     sys      - System Information Menu
     l2       - Layer 2 Information Menu
     l3       - Layer 3 Information Menu
     qos      - QoS Menu
     acl      - Show ACL information
     rmon     - Show RMON information
     link     - Show link status
     port     - Show port information
     transcvr - Show Port Transceiver status
     virt     - Show Virtualization information
     cee      - CEE Information Menu
     fcoe     - Fiber Channel Over Ethernet Information Menu
     swkey    - Show enabled software features
     dump     - Dump all information
```

The information provided by each menu option is briefly described in Table 5, with pointers to detailed information.

Table 5. Information Menu Options (/info)

Command Syntax and Usage
`sys` Displays the System Information Menu. For details, see page 19.
`l2` Displays the Layer 2 Information Menu. For details, see page 31.
`l3` Displays the Layer 3 Information Menu. For details, see page 54.
`qos` Displays the Quality of Service (QoS) Information Menu. For details, see page 88.
`acl` Displays the current configuration profile for each Access Control List (ACL) and ACL Group. For details, see page 90.
`rmon` Displays the Remote Monitoring (RMON) Information Menu. For details, see page 91.

Table 5. Information Menu Options (/info)

Command Syntax and Usage
`link` Displays configuration information about each port, 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 95.
`port` 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 – Fast Fowarding status – FDB Learning status – Flooding status For details, see page 96.
`transcvr` Displays the status of the port transceiver module on each external port. For details, see page 97.
`virt` Displays the Virtualization information menu. For details, see page 98.
`cee` Displays the Converged Enhanced Ethernet (CEE) information menu. For details, see page 103.
`fcoe` Displays the Fiber Channel over Ethernet (FCoE) information menu. For details, see page 111.
`swkey` Displays the enabled software features.
`dump` Dumps all switch information available from the Information Menu (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.

/info/sys

System Information Menu

```
[System Menu]
     errdis    - Errdisable Menu
     snmpv3    - SNMPv3 Information Menu
     chassis   - Show BladeCenter Chassis related information
     general   - Show general system information
     log       - Show last 100 syslog messages
     user      - Show current user status
     dump      - Dump all system information
```

The information provided by each menu option is briefly described in Table 6, with pointers to where detailed information can be found.

Table 6. System Menu Options (/info/sys)

Command Syntax and Usage
`errdis` Displays Error Disable and Recovery Information menu. To view the menu options, see page 20.
`snmpv3` Displays SNMPv3 Information Menu. To view the menu options, see page 20.
`chassis` Displays information about the Flex System chassis. For details, see page 27.
`general` 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 For details, see page 29.
`log` Displays most recent syslog messages. For details, see page 30.
`user` Displays configured user names and their status. For details, see page 30.
`dump` Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).

/info/sys/errdis

Error Disable and Recovery Information

```
[ErrDisable Information Menu]
     recovery - Show ErrDisable recovery information
     timers   - Show ErrDisable timer information
     dump     - Show all of the above
```

This menu allows you to display information about the Error Disable and Recovery feature for interface ports.

Table 7. Error Disable Information Options

Command Syntax and Usage
`recovery` Displays a list ports with their Error Recovery status.
`timers` Displays a list of active recovery timers, if applicable.
`dump` Displays all Error Disable and Recovery information.

/info/sys/snmpv3

SNMPv3 System Information Menu

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.

```
[SNMPv3 Information Menu]
     usm      - Show usmUser table information
     view     - Show vacmViewTreeFamily table information
     access   - Show vacmAccess table information
     group    - Show vacmSecurityToGroup table information
     comm     - Show community table information
     taddr    - Show targetAddr table information
     tparam   - Show targetParams table information
     notify   - Show notify table information
     dump     - Show all SNMPv3 information
```

Table 8. SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
`usm` Displays User Security Model (USM) table information. To view the table, see page 21.
`view` Displays information about view, sub-trees, mask and type of view. To view a sample, see page 22.
`access` Displays View-based Access Control information. To view a sample, see page 22.
`group` Displays information about the group that includes, the security model, user name, and group name. To view a sample, see page 23.
`comm` Displays information about the community table information. To view a sample, see page 24.
`taddr` Displays the Target Address table information. To view a sample, see page 24.
`tparam` Displays the Target parameters table information. To view a sample, see page 25.
`notify` Displays the Notify table information. To view a sample, see page 26.
`dump` Displays all the SNMPv3 information. To view a sample, see page 27.

/info/sys/snmpv3/usm

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 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 (/info/sys/usm)

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.

/info/sys/snmpv3/view

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.

```
View Name            Subtree               Mask           Type
-----------------    ------------------   --------------  --------
iso                  1.3                                   included
v1v2only             1.3                                   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 (/info/sys/snmpv3/view)

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.

/info/sys/snmpv3/access

SNMPv3 Access Table Information

The access control sub system 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.

Table 11. SNMPv3 Access Table Information (/info/sys/snmpv3/access)

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.

/info/sys/snmpv3/group

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.

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

Table 12. SNMPv3 Group Table Information Parameters (/info/sys/snmpv3/group)

Field	Description
Sec Model	Displays the security model used, which is any one of: USM, SNMPv1, SNMPv2, and SNMPv3.

Table 12. SNMPv3 Group Table Information Parameters (/info/sys/snmpv3/group)

Field	Description
User Name	Displays the name for the group.
Group Name	Displays the access name of the group.

/info/sys/snmpv3/comm

SNMPv3 Community Table Information

This command displays the community table information stored in the SNMP engine.

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

Table 13. SNMPv3 Community Table Parameters (/info/sys/snmpv3/comm)

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.

/info/sys/snmpv3/taddr

SNMPv3 Target Address Table Information

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 (/info/sys/snmpv3/taddr)

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.

Table 14. SNMPv3 Target Address Table Information Parameters (/info/sys/snmpv3/taddr)

Field	Description
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.

/info/sys/snmpv3/tparam

SNMPv3 Target Parameters Table Information

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

This command displays the SNMPv3 target parameters table information.

Table 15. SNMPv3 Target Parameters Table Information (/info/sys/snmpv3/tparam)

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.

/info/sys/snmpv3/notify

SNMPv3 Notify Table Information

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

This command displays the SNMPv3 notify table information.

Table 16. SNMPv3 Notify Table Information (/info/sys/snmpv3/notify)

Field	Description
Name	The locally arbitrary, but unique identifier associated with this `snmpNotifyEntry`.
Tag	This represents a single tag value that 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.

/info/sys/snmpv3/dump

SNMPv3 Dump Information

```
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                  1.3                               included
v1v2only             1.3                               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        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
-------------------- -------- ------------------  --------- -------
```

info/sys/chassis

Flex System Chassis Information

```
IBM Flex System Chassis Related Information:
    Switch Module Bay         = 1
    Chassis Type              = BladeCenter E
    Chassis UUID              = 00000000000000000000000000000000
    POST Results              = 0xff

    Management Module Control -

        Default Configuration         = FALSE
        Skip Extended Memory Test     = TRUE
        Disable External Ports        = FALSE
        POST Diagnostics Control      = Normal Diagnostics

        Control Register              = 0x39
        Extended Control Register     = 0x00

    Management Module Status Reporting -

        Device PowerUp Complete       = TRUE
        Over Current Fault            = FALSE
        Fault LED                     = OFF
        Primary Temperature Warning   = OK
        Secondary Temperature Warning = OK

        Status Register               = 0x40
        Extended Status Register      = 0x01
```

Chassis information includes details about the chassis type and position, and management module settings.

/info/sys/general

General System Information

```
System Information at 0:16:42 Wed Jan 3, 2012
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

IBM Flex System Fabric CN4093 10Gb Converged Scalable Switch

Switch has been up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot:  0:00:47 Wed Jan  3, 2012 (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):
Software Version 7.5.0 (FLASH image2), active configuration.


Hardware Part Number:  46C7193
Hardware Revision:     05
Serial Number:         PROTO2C04E
Manufacturing Date:    43/08
PCBA Part Number:      BAC-00072-00
PCBA Revision:         0
PCBA Number:           00
Board Revision:        05
PLD Firmware Version:  1.3

Temperature Warning:   26 C (Warn at 60 C/Recover at 55 C)
Temperature Shutdown:  27 C (Shutdown at 65 C/Recover at 60 C)
Temperature Inlet:     23 C
Temperature Exhaust:   26 C

Power Consumption:     42.570 W (12.000 V,  3.543 A)

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

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

System information includes:

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

/info/sys/log

Show Recent Syslog Messages

```
Date    Time      Criticality level       Message
Jul  8  17:25:41    NOTICE       system: link up on port INTA1
Jul  8  17:25:41    NOTICE       system: link up on port INTA8
Jul  8  17:25:41    NOTICE       system: link up on port INTA7
Jul  8  17:25:41    NOTICE       system: link up on port INTA2
Jul  8  17:25:41    NOTICE       system: link up on port INTA1
Jul  8  17:25:41    NOTICE       system: link up on port INTA4
Jul  8  17:25:41    NOTICE       system: link up on port INTA3
Jul  8  17:25:41    NOTICE       system: link up on port INTA6
Jul  8  17:25:41    NOTICE       system: link up on port INTA5
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 INTA3
Jul  8  17:25:42    NOTICE       system: link up on port INTA2
Jul  8  17:25:42    NOTICE       system: link up on port INTA4
Jul  8  17:25:42    NOTICE       system: link up on port INTA3
Jul  8  17:25:42    NOTICE       system: link up on port INTA6
Jul  8  17:25:42    NOTICE       system: link up on port INTA5
Jul  8  17:25:42    NOTICE       system: link up on port INTA1
Jul  8  17:25:42    NOTICE       system: link up on port INTA6
```

Each syslog message has a criticality 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 that the administrator is being notified of, as shown below.

- `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

/info/sys/user

User Status Information

```
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.

/info/l2

Layer 2 Information Menu

```
[Layer 2 Menu]
     fdb      - Forwarding Database Information Menu
     lacp     - Link Aggregation Control Protocol Menu
     failovr  - Show Failover information
     hotlink  - Show Hot Links information
     ecp      - ECP Information Menu
     lldp     - LLDP Information Menu
     udld     - UDLD Information Menu
     oam      - OAM Information Menu
     vlag     - vLAG Information Menu
     8021x    - Show 802.1X information
     stg      - Show STP information
     cist     - Show CIST information
     trunk    - Show Trunk Group information
     vlan     - Show VLAN information
     pvlan    - Show protocol VLAN information
     prvlan   - Show private-vlan information
     dump     - Dump all layer 2 information
```

The information provided by each menu option is briefly described in Table 17, with pointers to where detailed information can be found.

Table 17. Layer 2 Information Menu Options (/info/l2)

Command Syntax and Usage
`fdb` Displays the Forwarding Database Information Menu. For details, see page 33.
`lacp` Displays the Link Aggregation Control Protocol Menu. For details, see page 35.
`failovr` Displays the Layer 2 Failover Information menu. For details, see page 36.
`hotlink` Displays the Hot Links Information menu. For details, see page 37.
`ecp` Displays the Edge Control Protocol (ECP) Information menu. For details, see page 38.
`lldp` Displays the LLDP Information menu. For details, see page 38.
`udld` Displays the Unidirectional Link Detection (UDLD) Information menu. For details, see page 41.
`oam` Displays the Operation, Administration, and Maintenance (OAM) Information menu. For details, see page 42.

Table 17. Layer 2 Information Menu Options (/info/l2)

Command Syntax and Usage
`vlag` Displays the vLAG Information Menu. For details, see page 43.
`8021x` Displays the 802.1X Information Menu. For details, see page 44.
`stg` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (PVRST, RSTP, or MSTP), and VLAN membership. In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: – Priority – Hello interval – Maximum age value – Forwarding delay – Aging time You can also see the following port-specific STG information: – Port alias and priority – Cost – State For details, see page 46.
`cist` Displays Common Internal Spanning Tree (CIST) information, including the MSTP digest and VLAN membership. CIST bridge information includes: – Priority – Hello interval – Maximum age value – Forwarding delay – Root bridge information (priority, MAC address, path cost, root port) CIST port information includes: – Port number and priority – Cost – State For details, see page 50.
`trunk` When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see page 52.

Table 17. Layer 2 Information Menu Options (/info/l2)

Command Syntax and Usage
`vlan` Displays VLAN configuration information, including: – VLAN Number – VLAN Name – Status – Port membership of the VLAN For details, see page 52.
`pvlan` Displays Protocol VLAN information.
`prvlan` Displays Private VLAN information.
`dump` Dumps all switch information available from the Layer 2 menu (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.

`/info/l2/fdb`

FDB Information Menu

```
[Forwarding Database Menu]
      find    - Show a single FDB entry by MAC address
      port    - Show FDB entries on a single port
      trunk   - Show FDB entries on a single trunk
      vlan    - Show FDB entries on a single VLAN
      state   - Show FDB entries by state
      mcdump  - Show FDB multicast entries
      static  - Show FDB static entries
      dump    - Show all FDB entries
```

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 18. FDB Information Menu Options (/info/l2/fdb)

Command Syntax and Usage
`find` *<MAC address>* [*<VLAN>*] 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`
`port` *<port number or alias>* Displays all FDB entries for a particular port.
`trunk` *<trunk number>* Displays all FDB entries for a particular trunk.
`vlan` *<VLAN number>* Displays all FDB entries on a single VLAN.
`state unknown|forward|trunk` Displays all FDB entries of a particular state.
`mcdump` Displays all Multicast MAC entries in the FDB.
`static` Displays all static MAC entries in the FDB.
`dump` Displays all entries in the Forwarding Database. For more information, see page 34.

/info/l2/fdb/dump

Show All FDB Information

```
      MAC address     VLAN  Port  Trnk  State  Permanent
  ----------------  ----  ----  ----  -----  ---------
  00:04:38:90:54:18     1  EXT4         FWD
  00:09:6b:9b:01:5f     1  INTA13       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 which 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 Menu” on page 466.

/info/l2/lacp
Link Aggregation Control Protocol Information Menu

```
[LACP Menu]
     aggr     - Show LACP aggregator information
     port     - Show LACP port information
     dump     - Show all LACP ports information
```

Use these commands to display Link Aggregation Protocol (LACP) status information about each port on the switch.

Table 19. LACP Information Options (/info/l2/lacp)

Command Syntax and Usage
`aggr` *<aggregator ID>* Displays detailed information about the LACP aggregator.
`port` Displays LACP information about the selected port.
`dump` Displays a summary of LACP information. For details, see page 35.

/info/l2/lacp/dump
Show All LACP Information

```
port   mode     adminkey  operkey  selected   prio  aggr  trunk  status
------------------------------------------------------------------------
INTA1  active         30       30     yes    32768    17     19    up
INTA2  active         30       30     yes    32768    17     19    up
INTA3  off             3        3     no     32768    --     --    --
INTA4  off             4        4     no     32768    --     --    --
...
```

LACP dump includes the following information for each external port in the CN4093:

- `mode` Displays the port’s LACP mode (active, passive, or off).
- `adminkey` Displays the value of the port’s *adminkey*.
- `operkey` Shows the value of the port’s operational key.
- `selected` Indicates whether the port has been selected to be part of a Link Aggregation Group.

- `prio` Shows the value of the port priority.
- `aggr` Displays the aggregator associated with each port.
- `trunk` This value represents the LACP trunk group number.
- `status` Displays the status of LACP on the port (up or down).

/info/l2/failovr
Layer 2 Failover Information Menu

```
[Failover Info Menu]
     trigger  - Show Trigger information
```

Table 20 describes the Layer 2 Failover information options.

Table 20. Failover Information Options (/info/l2/failovr)

Command Syntax and Usage
`trigger` *<trigger number>* Displays detailed information about the selected Layer 2 Failover trigger.

/info/l2/failovr/trigger *<trigger number>*
Show Layer 2 Failover Information

```
Trigger 1 Auto Monitor: Enabled
Trigger 1 limit: 0
Monitor State: Up
Member      Status
---------   -----------
trunk 1
 EXT2       Operational
 EXT3       Operational

Control State: Auto Disabled
Member      Status
---------   -----------
 INTA1      Operational
 INTA2      Operational
 INTA3      Operational
 INTA4      Operational
...
```

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

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

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

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

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

/info/l2/hotlink
Hot Links Information Menu

```
[Hot Links Info Menu]
     trigger  - Show Trigger information
```

Table 21. Hot Links Information Options (/info/l2/hotlink)

Command Syntax and Usage
`trigger` Displays status and configuration information for each Hot Links trigger. To view a sample display, see page 37.

/info/l2/hotlink/trigger
Hotlinks Trigger Information

```
Hot Links Info: Trigger

Current global Hot Links setting: ON
bpdu disabled
sndfdb disabled

Current Trigger 1 setting: enabled
name "Trigger 1", preempt enabled, fdelay 1 sec

Active state: None

Master settings:
port EXT1
Backup settings:
port EXT2
```

Hot Links trigger information includes the following:

- Hot Links status (on or off)
- Status of BPDU flood option
- Status of FDB send option
- Status and configuration of each Hot Links trigger

/info/l2/ecp
ECP Information

```
[ECP Information Menu]
     channels - Show all ECP channels
     ulps     - Show all Registered ULPs
```

Table 22. ECP Information Options

Command Syntax and Usage
`channels` Displays all Edge Control Protocol (ECP) channels.
`ulps` Displays all registered Upper-Level Protocols (ULPs).

/info/l2/lldp
LLDP Information Menu

```
[LLDP Information Menu]
     port     - Show LLDP port information
     rx       - Show LLDP receive state machine information
     tx       - Show LLDP transmit state machine information
     remodev  - Show LLDP remote devices information
     dump     - Show all LLDP information
```

Table 23. LLDP Information Menu Options (/info/l2/lldp)

Command Syntax and Usage
`port` *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information. For more information, see page 38.
`rx` Displays information about the LLDP receive state machine.
`tx` Displays information about the LLDP transmit state machine.
`remodev` Displays information received from LLDP -capable devices. To view a sample display, see page 40.
`dump` Displays all LLDP information.

/info/l2/lldp/port

LLDP Port Information

```
[Show LLDP port information]
     tlv      - Optional TLVs Menu
     dump     - Show LLDP port information
```

Table 24. LLDP Information Options

Command Syntax and Usage
`tlv` Displays LLDP type-length-value (TLV) information for the port. For more information, see page 39.
`dump` Displays all LLDP information for the port.

/info/l2/lldp/port <*port no.*>/tlv

LLDP Port TLV Information

```
[Optional TLVs Menu]
     evb      - Show EVB TLV information
     dump     - Show all TLVs information
```

Table 25. LLDP Information Options

Command Syntax and Usage
`evb` Displays Edge Virtual Bridge (EVB) type-length-value (TLV) information.
`dump` Displays all TLV information for the port.

/info/l2/lldp/remodev

LLDP Remote Device Information

```
LLDP Remote Devices Information

LocalPort | Index | Remote Chassis ID | RemotePort | Remote System Name
----------|-------|-------------------|------------|---------------------------
     MGT1 | 210   | 00 16 ca ff 7e 00 | 15         | BNT Gb Ethernet Switch...
     EXT4 | 12    | 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, follow the `remodev` 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 CN4093 10Gb Converged
Scalable Switch, IBM Networking OS: version 7.5.0,45 Boot image: version 7.5.0.45

        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   :
```

/info/l2/udld
Unidirectional Link Detection Information Menu

```
[UDLD Information Menu]
     port     - Show UDLD port information
     dump     - Show all UDLD information
```

Table 26. UDLD Information Menu Options (/info/l2/udld)

Command Syntax and Usage
port *<port alias or number>* Displays UDLD information about the selected port. To view a sample display, see page 41.
dump Displays all UDLD information.

/info/l2/udld/port *<port alias or number>*
UDLD Port Information

```
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)

/info/l2/oam
OAM Discovery Information Menu

```
[OAM Information Menu]
     port     - Show OAM port information
     dump     - Show all OAM information
```

Table 27. OAM Discovery Information Menu Options (/info/l2/oam)

Command Syntax and Usage
port *<port alias or number>* Displays OAM information about the selected port. To view a sample display, see page 42.
dump Displays all OAM information.

/info/l2/oam/port *<port alias or number>*
OAM Port Information

```
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.

/info/l2/vlag

vLAG Information

```
[vLAG Information Menu]
     lacp     - Show LACP trunk information
     trunk    - Show Trunk Group information
     isl      - Show all vLAG ISL information
     dump     - Show all vLAG information
```

The following table describes the vLAG information parameters.

Table 28. vLAG Information Menu Options

Command Syntax and Usage
`lacp` Displays LACP trunk information.To view a sample display, see page 43.
`trunk` *<trunk group number>* Displays vLAG Trunk Group information. To view a sample display, see page 44.
`isl` Displays vLAG ISL information.
`dump` Displays all vLAG information.

/info/l2/vlag/lacp

vLAG LACP Information

```
[LACP Information Menu]
     l-aggr   - Show LACP aggregator information
     l-port   - Show LACP port information
     dump     - Show all vLAG information
```

Table 29. vLAG LACP Information Options

Command Syntax and Usage
`l-aggr` *<port alias or number>* Displays information about local vLAG LACP aggregators.
`l-port` *<port alias or number>* Displays information about local vLAG LACP ports.
`dump` Displays all vLAG information.

/info/l2/vlag/trunk

vLAG Information

```
vLAG is enabled on trunk 3
Protocol - Static
Current settings: enabled
    ports:  60
Current L2 trunk hash settings:
    smac
Current L3 trunk hash settings:
    sip dip
Current ingress port hash: disabled
Current L4 port hash: disabled
```

/info/l2/8021x

802.1X Information

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
Guest VLAN status : disabled
Guest VLAN        : none
                                    Authenticator    Backend   Assigned
Port    Auth Mode    Auth Status     PAE State     Auth State   VLAN
-----  -----------  ------------  --------------  ---------- --------
*INTA1 force-auth    unauthorized  initialize      initialize   none
*INTB1 force-auth    unauthorized  initialize      initialize   none
*INTC1 force-auth    unauthorized  initialize      initialize   none
*INTA2 force-auth    unauthorized  initialize      initialize   none
*INTB2 force-auth    unauthorized  initialize      initialize   none
*INTC2 force-auth    unauthorized  initialize      initialize   none
...
*EXT1  force-auth    unauthorized  initialize      initialize   none
*EXT2  force-auth    unauthorized  initialize      initialize   none
*EXT3  force-auth    unauthorized  initialize      initialize   none
*EXT4  force-auth    unauthorized  initialize      initialize   none
...
------------------------------------------------------------------
* - Port down or disabled
```

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

The following table describes the IEEE 802.1X parameters.

Table 30. 802.1X Parameter Descriptions (/info/l2/8021x)

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: • `force-unauth` • `auto` • `force-auth`
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: • `initialize` • `disconnected` • `connecting` • `authenticating` • `authenticated` • `aborting` • `held` • `forceAuth`
Backend Auth State	Displays the Backend Authorization State. The Backend Authorization state can be one of the following: • `initialize` • `request` • `response` • `success` • `fail` • `timeout` • `idle`

/info/l2/stg

Spanning Tree Information

```
-------------------------------------------------------------------
Pvst+ compatibility mode enabled
-------------------------------------------------------------------
Spanning Tree Group 1: On (PVRST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 ffff 00:13:0a:4f:7d:d0        0    EXT2    2     20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging  Topology Change Counts
              65535      2      20      15     300                0

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
INTA1  128     2000!  FWD   ROOT 8000-00:22:00:ee:cc:00     8001  P2P
INTA2  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8002  P2P
INTA3  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8003  P2P
...
EXT1  128     2000!  DISC  DESG 8001-00:22:00:7d:5f:00     800a  P2P
EXT2  128     2000!  DISC  DESG 8001-00:22:00:7d:5f:00     800b  P2P
...
! = Automatic path cost.

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

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

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

The switch software uses the Per VLAN Rapid Spanning Tree Protocol (PVRST) Spanning Tree mode, with IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), as alternatives. For details see "RSTP/MSTP/PVRST Information" on page 48.

When STP is enabled, in addition to seeing if STG is enabled or disabled, you can view the following STG bridge information:

Table 31. Spanning Tree Bridge Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root.
Priority (bridge)	The Bridge Priority parameter controls which bridge on the network will become the STG root bridge.

Table 31. Spanning Tree Bridge Parameter Descriptions (continued)

Parameter	Description
Hello	The Hello Time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STG network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

The following port-specific information is also displayed:

Table 32. Spanning Tree Port Parameter Descriptions

Parameter	Description
Priority (port)	The Port Priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The Port Path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The State field shows the current state of the port. The state field can be `FWD` (Forwarding), `DISC` (Discarding) or `LRN` (Learning).
Role	The role field shows the current role of the port: DESG (Designated), `ROOT` (Root Port), `ALTN` (Alternate) or `BKUP` (Backup).
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The Designated Port field shows the port on the Designated Bridge to which this port is connected.

/info/l2/stg

RSTP/MSTP/PVRST Information

```
Spanning Tree Group 1: On (RSTP)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel
 ffff 00:13:0a:4f:7d:d0        0    EXT4     2    20     15

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              61440      2      20      15     300

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
INTA1  128     2000!  FWD   ROOT 8000-00:22:00:ee:cc:00     8001  P2P
INTA2  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8002  P2P
INTA3  128     2000!  DISC  ALTN 8000-00:22:00:ee:cc:00     8003  P2P
...
EXT1   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8011     P2P
EXT2   128      2000  DISC  BKUP 8000-00:11:58:ae:39:00    8011     P2P
EXT3   128      2000  FWD   DESG 8000-00:11:58:ae:39:00    8013     P2P
EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8013  Shared
EXT5   128      2000  FWD
...
------------------------------------------------------------------
Spanning Tree Group 128: Off (RSTP), FDB aging timer 300
VLANs:  4095

Port  Prio  Cost     State  Role Designated Bridge      Des Port Type
----- ---- --------- -----  ---- ---------------------- -------- ----
EXTM            0        0    FWD *
MGT1            0        0    FWD *

* = STP turned off for this port.
```

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

The switch software can be set to use the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) or the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). If RSTP/MSTP is turned on (see page 274), you can view RSTP/MSTP bridge information for the Spanning Tree Group and port-specific RSTP information.

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

Table 33. RSTP/MSTP/PVRST Bridge Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (in hexadecimal notation) and the MAC address of the root.
Priority (bridge)	The Bridge Priority parameter controls which bridge on the network will become the STP root bridge.

Table 33. RSTP/MSTP/PVRST Bridge Parameter Descriptions (continued)

Parameter	Description
Hello	The Hello Time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The Maximum Age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
FwdDel	The Forward Delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from listening to learning and from learning state to forwarding state.
Aging	The Aging Time parameter specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

The following port-specific information is also displayed:

Table 34. RSTP/MSTP/PVRST Port Parameter Descriptions

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

Table 34. RSTP/MSTP/PVRST Port Parameter Descriptions (continued)

Parameter	Description
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are AUTO, P2P, or SHARED.

/info/l2/cist

Common Internal Spanning Tree Information

```
Common Internal Spanning Tree: on
VLANs:  2-4094

Current Root:            Path-Cost  Port MaxAge FwdDel
 8000 00:11:58:ae:39:00        0       0     20     15

Cist Regional Root:       Path-Cost
 8000 00:11:58:ae:39:00        0

Parameters:  Priority  MaxAge  FwdDel  Hops
              61440      20      15    20
Port  Prio  Cost     State  Role Designated Bridge      Des Port Hello Type
----- ---- --------- -----  ---- ---------------------- -------- ----- ----
 INTA1    0         0  DSB *
 INTA2    0         0  DSB *
 INTA3    0         0  FWD *
 INTA4    0         0  DSB *
 INTA5    0         0  DSB *
 INTA6    0         0  DSB *
 INTA7    0         0  DSB *
 INTA8    0         0  DSB *
 INTA9    0         0  DSB *
 INTA10   0         0  DSB *
 INTA11   0         0  DSB *
 INTA12   0         0  DSB *
 INTA13   0         0  DSB *
 INTA14   0         0  DSB *
 MGT1     0         0  FWD *
*EXT1   128     20000  FWD   DESG 8000-00:11:58:ae:39:00    8011   2    P2P
 EXT2   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8011   2    P2P
 EXT3   128     20000  FWD   DESG 8000-00:11:58:ae:39:00    8013   2    P2P
 EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8013   2    Shared
...
* = STP turned off for this port.
```

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

In addition to seeing if Common Internal Spanning Tree (CIST) is enabled or disabled, you can view CIST bridge and port-specific information. The following table describes the CIST parameters.

Table 35. CIST Parameter Descriptions

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Hops	The maximum number of bridge hops a packet can traverse before it is dropped. The default value is 20.
Priority (port)	The port priority parameter helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	The state field shows the current state of the port. The state field can be either Discarding (`DISC`), Learning (`LRN`), or Forwarding (`FWD`).
Role	The Role field shows the current role of this port in the Spanning Tree. The port role can be one of the following: Designated (`DESG`), Root (`ROOT`), Alternate (`ALTN`), Backup (`BKUP`), Disabled (`DSB`), Master (`MAST`), or Unknown (`UNK`).

Table 35. CIST Parameter Descriptions

Parameter	Description
Designated Bridge	The Designated Bridge shows information about the bridge connected to each port, if applicable. Information includes the priority (in hexadecimal notation) and MAC address of the Designated Bridge.
Designated Port	The port ID of the port on the Designated Bridge to which this port is connected.
Type	Type of link connected to the port, and whether the port is an edge port. Link type values are `AUTO`, `P2P`, or `SHARED`.

/info/l2/trunk
Trunk Group Information

```
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`.

/info/l2/vlan
VLAN Information

```
VLAN                Name                Status MGT          Ports
----  --------------------------------  ------ --- -------------------------
1     Default VLAN                      ena    dis  INTA1-INTB14 EXT1-EXT10
                                                    EXT15-EXT22
4095  Mgmt VLAN                         ena    ena  MGT1 EXTM

Private-VLAN  Type       Mapped-To  Status     Ports
------------ --------- ---------- ---------- -----------------
1000          primary    1001-1014  ena         EXT1 EXT2
1001          isolated   1000       ena         INTA1
1002          community  1000       ena         INTA2
1003          community   1000       ena        INTA3
```

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

This information display includes all configured VLANs and all member ports that have an active link state. Port membership is represented in slot/port format.

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN
- Protocol-based VLAN information, if applicable
- Private VLAN configuration, if applicable

/info/l3

Layer 3 Information Menu

```
[Layer 3 Menu]
     route    - IP Routing Information Menu
     arp      - ARP Information Menu
     bgp      - BGP Information Menu
     ospf     - OSPF Routing Information Menu
     ospf3    - OSPFv3 Routing Information Menu
     rip      - RIP Routing Information Menu
     route6   - IP6 Routing Information Menu
     nbrcache - IP6 Neighbor Cache Information Menu
     ndprefix - IP6 Neighbour Discovery Information
     ecmp     - Show ECMP static routes information
     hash     - Show ECMP hashing result
     igmp     - Show IGMP Snooping Multicast Group information
     mld      - Show MLD information
     vrrp     - Show Virtual Router Redundancy Protocol information
     if       - Show Interface information
     ip6pmtu  - Show IPv6 Path MTU information
     ip       - Show IP information
     ikev2    - Show IKEv2 Information
     ipsec    - IPsec Information Menu
     dump     - Dump all layer 3 information
```

The information provided by each menu option is briefly described in Table 36, with pointers to detailed information.

Table 36. Layer 3 Information Options (/info/l3)

Command Syntax and Usage
`route` Displays the IP Routing Menu. Using the options of this menu, the system displays the following for each configured or learned route: – Route destination IP address, subnet mask, and gateway address – Type of route – Tag indicating origin of route – Metric for RIP tagged routes, specifying the number of hops to the destination (1-15 hops, or 16 for infinite hops) – The IP interface that the route uses For details, see page 56.
`arp` Displays the Address Resolution Protocol (ARP) Information Menu. For details, see page 58.
`bgp` Displays BGP Information Menu. To view menu options, see page 60.
`ospf` Displays OSPF routing Information Menu. For details, see page 63.
`ospf3` Displays OSPFv3 routing Information Menu. For details, see page 68.

Table 36. Layer 3 Information Options (/info/l3)

Command Syntax and Usage
`rip` Displays Routing Information Protocol Menu. For details, see page 73.
`route6` Displays the IPv6 Routing information menu. To view menu options, see page 74.
`nbrcache` Displays the IPv6 Neighbor Discovery cache information menu. To view menu options, see page 75.
`ndprefix` Displays the IPv6 Neighbor Discovery Prefix information menu. To view menu options, see page 76.
`ecmp` Displays information about ECMP static routes. For details, see page 76.
`hash` *<Source IP address> <destination IP address> <number of ECMP paths>* Displays information about ECMP hashing results. For details, see page 76.
`ip` Displays IP Information. For details, see page 85. 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
`igmp` Displays IGMP Information Menu. For details, see page 77.
`mld` Displays MLD Information Menu. For details, see page 81.
`vrrp` Displays VRRP Information. For details, see page 83.
`if` Displays interface information. For details, see page 83.
`ip6pmtu [`*<destination IPv6 address>*`]` Displays IPv6 Path MTU information. For details, see page 84.

Table 36. Layer 3 Information Options (/info/l3)

Command Syntax and Usage
`ip` Displays IP Information. For details, see page 85. 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
`ikev2` Displays IKEv2 Information menu. For details, see page 86.
`ipsec` Displays IPsec Information menu. For details, see page 87.
`dump` Dumps all switch information available from the Layer 3 menu (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.

/info/l3/route
IP Routing Information Menu

```
[IP Routing Menu]
      find    - Show a single route by destination IP address
      gw      - Show routes to a single gateway
      type    - Show routes of a single type
      tag     - Show routes of a single tag
      if      - Show routes on a single interface
      dump    - Show all routes
```

Using the commands listed in the following table, you can display all or a portion of the IP routes currently held in the switch.

Table 37. Route Information Menu Options (/info/l3/route)

Command Syntax and Usage
`find` *<IP address (such as 192.4.17.101)>* Displays a single route by destination IP address.
`gw` *<default gateway address (such as 192.4.17.44)>* Displays routes to a single gateway.
`type indirect|direct|local|broadcast|martian|multicast` Displays routes of a single type. For a description of IP routing types, see Table 38 on page 57.

Table 37. Route Information Menu Options (/info/l3/route)

Command Syntax and Usage
`tag fixed|static|addr|rip|ospf|bgp|broadcast| martian|multicast` Displays routes of a single tag. For a description of IP routing types, see Table 39 on page 58.
`if` *<interface number>* Displays routes on a single interface.
`dump` Displays all routes configured in the switch. For more information, see page 57.

/info/l3/route/dump

Show All IP Route Information

```
Status code: * - best
    Destination         Mask         Gateway        Type      Tag    Metr If
 --------------- --------------- --------------- --------- --------- ---- ---
* 12.0.0.0        255.0.0.0       11.0.0.1        direct    fixed         128
* 12.0.0.1        255.255.255.255 11.0.0.1        local     addr          128
* 12.255.255.255  255.255.255.255 11.255.255.255  broadcast broadcast     128
* 12.0.0.0        255.0.0.0       12.0.0.1        direct    fixed          12
* 12.0.0.1        255.255.255.255 12.0.0.1        local     addr           12
* 255.255.255.255 255.255.255.255 12.255.255.255  broadcast broadcast       2
* 224.0.0.0       224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.5       255.255.255.255 0.0.0.0         multicast addr
```

The following table describes the `Type` parameters.

Table 38. IP Routing Type Parameters

Parameter	Description
indirect	The next hop to the host or subnet destination will be forwarded through a router at the `Gateway` address.
direct	Packets will be delivered to a destination host or subnet attached to the switch.
local	Indicates a route to one of the switch's IP interfaces.
broadcast	Indicates a broadcast route.
martian	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
multicast	Indicates a multicast route.

The following table describes the `Tag` parameters.

Table 39. IP Routing Tag Parameters

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the CN4093.
addr	The address belongs to one of the switch's IP interfaces.
rip	The address was learned by the Routing Information Protocol (RIP).
ospf	The address was learned by Open Shortest Path First (OSPF).
bgp	The address was learned via Border Gateway Protocol (BGP)
broadcast	Indicates a broadcast address.
martian	The address belongs to a filtered group.
multicast	Indicates a multicast address.

/info/l3/arp
ARP Information Menu

```
[Address Resolution Protocol Menu]
      find    - Show a single ARP entry by IP address
      port    - Show ARP entries on a single port
      vlan    - Show ARP entries on a single VLAN
      addr    - Show ARP address list
      dump    - Show all ARP entries
```

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 40), VLAN and port for the address, and port referencing information.

Table 40. ARP Information Menu Options (/info/l3/arp)

Command Syntax and Usage
`find` *<IP address (such as, 192.4.17.101>* Displays a single ARP entry by IP address.
`port` *<port alias or number>* Displays the ARP entries on a single port.
`vlan` *<VLAN number>* Displays the ARP entries on a single VLAN.

Table 40. ARP Information Menu Options (/info/l3/arp)

Command Syntax and Usage
addr Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.
dump Displays all ARP entries. including: – IP address and MAC address of each entry – Address status flag (see below) – The VLAN and port to which the address belongs – The ports which have referenced the address (empty if no port has routed traffic to the IP address shown) For more information, see page 59.

/info/l3/arp/dump

Show All ARP Entry Information

```
    IP address     Flags    MAC address    VLAN  Age Port
---------------- ----- ----------------- ----  --- -----
12.20.1.1              00:15:40:07:20:42 4095    0  INT8
12.20.20.16            00:30:13:e3:44:14 4095    2  INT8
12.20.20.18            00:30:13:e3:44:14 4095    2  INT6
12.20.23.111           00:1f:29:95:f7:e5 4095    6  INT6
```

The `Port` field shows the target port of the ARP entry.

The `Flag` field is interpreted as follows:

Table 41. ARP Dump Flag Parameters

Flag	Description
P	Permanent entry created for switch IP interface.
R	Indirect route entry.
U	Unresolved ARP entry. The MAC address has not been learned.

/info/l3/arp/addr

ARP Address List Information

```
   IP address        IP mask        MAC address    VLAN Pass-Up
--------------- --------------- ----------------- ---- -------
205.178.18.66   255.255.255.255  00:70:cf:03:20:04
205.178.50.1    255.255.255.255  00:70:cf:03:20:06    1
205.178.18.64   255.255.255.255  00:70:cf:03:20:05    1
```

/info/l3/bgp

BGP Information Menu

```
[BGP Menu]
     peer     - Show all BGP peers
     summary  - Show all BGP peers in summary
     peerrt   - Show BGP peer routes
     dump     - Show BGP routing table
```

Table 42. BGP Peer Information Menu Options (/info/l3/bgp)

Command Syntax and Usage
`peer` Displays BGP peer information. See page 61 for a sample output.
`summary` Displays peer summary information such as AS, message received, message sent, up/down, state. See page 61 for a sample output.
`peerrt` Displays BGP peer routes. See page 61 for a sample output.
`dump` Displays the BGP routing table. See page 62 for a sample output.

/info/l3/bgp/peer

BGP Peer Information

Following is an example of the information that `/info/l3/bgp/peer` provides.

```
BGP Peer Information:

  3: 2.1.1.1         , version 4, TTL 225
    Remote AS: 100, Local AS: 100, Link type: IBGP
    Remote router ID: 3.3.3.3,    Local router ID: 1.1.201.5
    BGP status: idle, Old status: idle
    Total received packets: 0, Total sent packets: 0
    Received updates: 0, Sent updates: 0
    Keepalive: 60, Holdtime: 180, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 1

  4: 2.1.1.4         , version 4, TTL 225
    Remote AS: 100, Local AS: 100, Link type: IBGP
    Remote router ID: 4.4.4.4,    Local router ID: 1.1.201.5
    BGP status: idle, Old status: idle
    Total received packets: 0, Total sent packets: 0
    Received updates: 0, Sent updates: 0
    Keepalive: 60, Holdtime: 180, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 1
```

/info/l3/bgp/summary

BGP Summary Information

Following is an example of the information that `/info/l3/bgp/summary` provides.

```
   BGP Peer Summary Information:
        Peer         V    AS     MsgRcvd  MsgSent Up/Down   State
     --------------- - -------- -------- -------- -------- ----------
  1: 205.178.23.142  4      142      113      121 00:00:28 established
  2: 205.178.15.148  0      148        0        0 never     connect
```

/info/l3/bgp/peerrt

BGP Peer Routes Information

Following is an example of the information for BGP peer routes.

```
Current BGP neighbor 1 routes:
 Status codes: * valid, > best, = multipath, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Mask            Next Hop        Metric LcPrf  Wght  Path
   --------------- --------------- --------------- ------- ----- ----- ------------
*> 157.0.0.0       255.255.255.0   200.0.0.2         256    4    10     i
*> 157.0.1.0       255.255.255.0   200.0.0.2         256    4    10     i
*> 157.0.2.0       255.255.255.0   200.0.0.2         256    4    10     i
*> 157.0.3.0       255.255.255.0   200.0.0.2         256    4    10     i
*> 157.0.4.0       255.255.255.0   200.0.0.2         256    4    10     i
*> 157.0.5.0       255.255.255.0   200.0.0.2         256    4    10     i
```

/info/l3/bgp/dump

Show All BGP Information

Following is an example of the information that `/info/l3/bgp/dump` provides.

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

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

/info/l3/ospf

OSPF Information Menu

```
[OSPF Information Menu]
      general - Show general information
      aindex  - Show area(s) information
      if      - Show interface(s) information
      loopif  - Show loopback interface(s) information
      virtual - Show details of virtual links
      nbr     - Show neighbor(s) information
      dbase   - Database Menu
      sumaddr - Show summary address list
      nsumadd - Show NSSA summary address list
      routes  - Show OSPF routes
      dump    - Show OSPF information
```

Table 43. OSPF Information Menu Options (/info/l3/ospf)

Command Syntax and Usage
`general` Displays general OSPF information. See page 65 for a sample output.
`aindex` *<area index (0-2)>* Displays area information for a particular area index. If no parameter is supplied, it displays area information for all the areas.
`if` *<interface number>* Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See page 65 for a sample output.
`loopif` *<interface number>* Displays loopback information for a particular interface. If no parameter is supplied, it displays loopback information for all the interfaces. See page 65 for a sample output.
`virtual` Displays information about all the configured virtual links.
`nbr` *<nbr router-id (A.B.C.D)>* Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.
`dbase` Displays OSPF database menu. To view menu options, see page 65.
`sumaddr` *<area index (0-2)>* Displays the list of summary ranges belonging to non-NSSA areas.
`nsumadd` *<area index (0-2)>* Displays the list of summary ranges belonging to NSSA areas.

Table 43. OSPF Information Menu Options (/info/l3/ospf)

Command Syntax and Usage
`routes` Displays OSPF routing table. See page 68 for a sample output.
`dump` Displays the OSPF information.

/info/l3/ospf/general

OSPF General Information

```
OSPF Version 2
Router ID: 10.10.10.1
Started at 1663 and the process uptime is 4626
Area Border Router: yes, AS Boundary Router: no
LS types supported are 6
External LSA count 0
External LSA checksum sum 0x0
Number of interfaces in this router is 2
Number of virtual links in this router is 1
16 new lsa received and 34 lsa originated from this router
Total number of entries in the LSDB 10
Database checksum sum 0x0
Total neighbors are 1, of which
                                  2 are >=INIT state,
                                  2 are >=EXCH state,
                                  2 are =FULL state
Number of areas is 2, of which 3-transit 0-nssa
        Area Id : 0.0.0.0
        Authentication : none
        Import ASExtern : yes
        Number of times SPF ran : 8
        Area Border Router count : 2
        AS Boundary Router count : 0
        LSA count : 5
        LSA Checksum sum : 0x2237B
        Summary : noSummary
```

/info/l3/ospf/if *<interface number>*

OSPF Interface Information

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
   Router ID 10.10.10.1, State DR, Priority 1
   Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
   Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
   Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
   Neighbor count is 1   If Events 4, Authentication type none
```

/info/l3/ospf/loopif *<interface number>*

OSPF Interface Loopback Information

```
Ip Address 123.123.123.1, Area 0.0.0.0, Passive interface, Admin Status UP
   Router ID 1.1.1.1, State Loopback, Priority 1
   Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Backup Designated Router (ID) 0.0.0.0, Ip Address 0.0.0.0
   Timer intervals, Hello 10, Dead 40, Wait 40, Retransmit 5, Transit delay 1
   Neighbor count is 0   If Events 1, Authentication type none
```

/info/l3/ospf/dbase

OSPF Database Information Menu

```
[OSPF Database Menu]
      advrtr  - LS Database info for an Advertising Router
      asbrsum - ASBR Summary LS Database info
      dbsumm  - LS Database summary
      ext     - External LS Database info
      nw      - Network LS Database info
      nssa    - NSSA External LS Database info
      rtr     - Router LS Database info
      self    - Self Originated LS Database info
      summ    - Network-Summary LS Database info
      all     - All
```

Table 44. OSPF Database Information Menu Options (/info/l3/ospf/dbase)

Command Syntax and Usage
`advrtr` *<router-id (A.B.C.D)>* Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.
`asbrsum` *<adv-rtr (A.B.C.D)>* | *<link_state_id (A.B.C.D>* | *<self>* Displays ASBR summary LSAs. The usage of this command is as follows: – `asbrsum adv-rtr 20.1.1.1` Displays ASBR summary LSAs having the advertising router 20.1.1.1. – `asbrsum link-state-id 10.1.1.1` Displays ASBR summary LSAs having the link state ID 10.1.1.1. – `asbrsum self` Displays the self advertised ASBR summary LSAs. – `asbrsum` with no parameters displays all the ASBR summary LSAs.
`dbsumm` Displays the following information about the LS database in a table format: – Number of LSAs of each type in each area. – Total number of LSAs for each area. – Total number of LSAs for each LSA type for all areas combined. – Total number of LSAs for all LSA types for all areas combined. No parameters are required.
`ext` *<adv-rtr (A.B.C.D)>* | *<link_state_id (A.B.C.D>* | *<self>* Displays the AS-external (type 5) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
`nw` *<adv-rtr (A.B.C.D)>* | *<link_state_id (A.B.C.D>* | *<self>* Displays the network (type 2) LSAs with detailed information of each field of the LSA.network LS database. The usage of this command is the same as the usage of the command `asbrsum`.

Table 44. OSPF Database Information Menu Options (/info/l3/ospf/dbase)

Command Syntax and Usage
`nssa` *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the NSSA (type 7) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
`rtr` *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the router (type 1) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
`self` Displays all the self-advertised LSAs. No parameters are required.
`summ` *<adv-rtr (A.B.C.D)> | <link_state_id (A.B.C.D> | <self>* Displays the network summary (type 3) LSAs with detailed information of each field of the LSAs. The usage of this command is the same as the usage of the command `asbrsum`.
`all` Displays all the LSAs.

/info/l3/ospf/routes

OSPF Route Codes Information

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

/info/l3/ospf3

OSPFv3 Information Menu

```
[OSPFv3 Information Menu]
     aindex   - Show area database information Menu
     dbase    - Database Menu
     areas    - Show areas information
     if       - Show interface(s) information
     virtual  - Show details of virtual links
     nbr      - Show neighbor(s) information
     host     - Show host information
     reqlist  - Show request list
     retlist  - Show retransmission list
     sumaddr  - Show summary address information
     redist   - Show config applied to routes learnt from RTM
     ranges   - Show OSPFv3 summary ranges
     routes   - Show OSPFv3 routes
     borderrt - Show OSPFv3 routes to an abr/asbr
     dump     - Show OSPFv3 information
```

Table 45. OSPFv3 Information Menu Options (/info/l3/ospf3)

Command Syntax and Usage
`aindex` *<area index (0-2)>* Displays the area information menu for a particular area index. To view menu options, see page 70.
`dbase` Displays the OSPFv3 database menu. To view menu options, see page 71.
`areas` Displays the OSPFv3 Area Table.

Table 45. OSPFv3 Information Menu Options (/info/l3/ospf3)

Command Syntax and Usage
`if` *<interface number>* Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. To view a sample display, see page 71.
`virtual` Displays information about all the configured virtual links.
`nbr` *<nbr router-id (A.B.C.D)>* Displays the status of a neighbor with a particular router ID. If no router ID is supplied, it displays the information about all the current neighbors.
`host` Displays OSPFv3 host configuration information.
`reqlist` *<nbr router-id (A.B.C.D)>* Displays the OSPFv3 request list. If no router ID is supplied, it displays the information about all the current neighbors.
`retlist` *<nbr router-id (A.B.C.D)>* Displays the OSPFv3 retransmission list. If no router ID is supplied, it displays the information about all the current neighbors.
`sumaddr` Displays the OSPFv3 external summary-address configuration information.
`redist` Displays OSPFv3 redistribution information to be applied to routes learned from the route table.
`ranges` Displays the OSPFv3 list of all area address ranges information.
`routes` Displays OSPFv3 routing table. To view a sample display, see page 73.
`borderrt` Displays OSPFv3 routes to an ABR or ASBR.
`dump` Displays all OSPFv3 information. To view a sample display, see page 71.

/info/l3/ospf3/aindex <*0-2*>

OSPFv3 Area Index Information Menu

```
[Area Info Menu]
     asext    - External LS Database info
     interprf - Inter Area Prefix LS Database info
     interrtr - Inter Area Router LS Database info
     intraprf - Intra Area Prefix LS Database info
     link     - Link LS Database info
     network  - Network LS Database info
     rtr      - Router LS Database info
     nssa     - NSSA LS Database info
     all      - All
```

The following commands allow you to display database information about the specified area.

Table 46. OSPFv3 Area Index Information Options (/info/l3/ospf3/aindex)

Command Syntax and Usage
`asext [detail|hex]` Displays AS-External LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`interprf [detail|hex]` Displays Inter-Area Prefix LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`interrtr [detail|hex]` Displays Inter-Area router LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`intraprf [detail|hex]` Displays Intra-Area Prefix LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`link [detail|hex]` Displays Link LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`network [detail|hex]` Displays Network LSAs database information for the selected area. If no parameter is supplied, it displays condensed information.
`rtr [detail|hex]` Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.
`nssa [detail|hex]` Displays NSSA database information for the selected area. If no parameter is supplied, it displays condensed information.
`all [detail|hex]` Displays all the LSAs for the selected area. If no parameter is supplied, it displays condensed information.

/info/l3/ospf3/dump

OSPFv3 Information

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

/info/l3/ospf3/if *<interface number>*

OSPFv3 Interface Information

```
       Ospfv3 Interface Information

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

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

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

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

/info/l3/ospf3/dbase

OSPFv3 Database Information Menu

```
[OSPFv3 Database Menu]
     asext    - External LS Database info
     interprf - Inter Area Prefix LS Database info
     interrtr - Inter Area Router LS Database info
     intraprf - Intra Area Prefix LS Database info
     link     - Link LS Database info
     network  - Network LS Database info
     rtr      - Router LS Database info
     nssa     - NSSA LS Database info
     all      - All
```

Table 47. OSPFv3 Database Information Options (/info/l3/ospf3/dbase)

Command Syntax and Usage
`asext` <*detail*>|<*hex*> Displays AS-External LSAs database information. If no parameter is supplied, it displays condensed information.
`interprf` <*detail*>|<*hex*> Displays Inter-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.
`interrtr` <*detail*>|<*hex*> Displays Inter-Area router LSAs database information. If no parameter is supplied, it displays condensed information.
`intraprf` <*detail*>|<*hex*> Displays Intra-Area Prefix LSAs database information. If no parameter is supplied, it displays condensed information.
`link` <*detail*>|<*hex*> Displays Link LSAs database information. If no parameter is supplied, it displays condensed information.
`network` <*detail*>|<*hex*> Displays Network LSAs database information. If no parameter is supplied, it displays condensed information.
`rtr` <*detail*>|<*hex*> Displays the Router LSAs with detailed information of each field of the LSAs. If no parameter is supplied, it displays condensed information.
`nssa` <*detail*>|<*hex*> Displays Type-7 (NSSA) LSA database information. If no parameter is supplied, it displays condensed information.
`all` <*detail*>|<*hex*> Displays all the LSAs. If no parameter is supplied, it displays condensed information.

/info/l3/ospf3/routes

OSPFv3 Route Codes Information

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

/info/l3/rip

Routing Information Protocol Information Menu

```
[RIP Information Menu]
     routes    - Show RIP routes
     dump      - Show RIP user's configuration
```

Use this menu to view information about the Routing Information Protocol (RIP) configuration and statistics.

Table 48. RIP Information Menu Options (/info/l3/rip)

Command Syntax and Usage
routes Displays RIP routes. For more information, see page 73.
dump *<interface number or zero for all IFs)>* Displays RIP user's configuration. For more information, see page 74.

/info/l3/rip/routes

RIP Routes Information

```
>> IP Routing# /info/l3/rip/routes

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

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

/info/l3/rip/dump <*interface number*>

Show RIP Interface Information

```
RIP USER CONFIGURATION :
        RIP ON update 30
        RIP on Interface 1 : 10.4.4.2,         enabled
        version 2, listen enabled, supply enabled, default none
        poison disabled, split horizon enabled, trigg enabled,
        mcast enabled, metric 1
        auth none,key none
```

/info/l3/route6

IPv6 Routing Information Menu

```
[IP6 Routing Menu]
     find     - Show a single route by destination IP address
     gw       - Show routes to a single next hop
     type     - Show routes of a single type
     if       - Show routes on a single interface
     summ     - Show routes summary
     dump     - Show all routes
```

Table 49 describes the IPv6 Routing information options.

Table 49. IPv6 Routing Information Menu Options (/info/l3/route6)

Command Syntax and Usage
`find` <*IP address (such as 3001:0:0:0:0:0:abcd:12)*> Displays a single route by destination IP address.
`gw` <*default gateway address (such as 3001:0:0:0:0:0:abcd:14)*> Displays routes to a single gateway.
`type connected|static|ospf` Displays routes of a single type. For a description of IP routing types, see Table 38 on page 57.
`if` <*interface number*> Displays routes on a single interface.
`summ` Displays a summary of IPv6 routing information, including inactive routes.
`dump` Displays all IPv6 routing information. For more information, see page 75.

/info/l3/route6/dump

IPv6 Routing Table Information

```
IPv6 Routing Table - 3 entries
Codes : C - Connected, S - Static
        O - OSPF

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

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

/info/l3/nbrcache

IPv6 Neighbor Discovery Cache Information Menu

```
[IP6 Neighbor Discovery Protocol Menu]
     find     - Show a single NBR Cache entry by IP address
     port     - Show NBR Cache entries on a single port
     vlan     - Show NBR Cache entries on a single VLAN
     dump     - Show all NBR Cache entries
```

Table 50 describes IPv6 Neighbor Discovery cache information menu options.

Table 50. IPv6 Neighbor Discovery Cache Information Options (/info/l3/nbrcache)

Command Syntax and Usage
`find` *<IPv6 address>* Shows a single Neighbor Discovery cache entry by IP address.
`port` *<port alias or number>* Shows the Neighbor Discovery cache entries on a single port.
`vlan` *<VLAN number>* Shows the Neighbor Discovery cache entries on a single VLAN.
`dump` Shows all Neighbor Discovery cache entries. For more information, see page 76.

/info/l3/nbrcache/dump

IPv6 Neighbor Discovery Cache Information

```
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
```

/info/l3/ndprefix

IPv6 Neighbor Discovery Prefix Information

```
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.

/info/l3/ecmp

ECMP Static Routes Information

```
Current ecmp static routes:
  Destination     Mask            Gateway         If    GW Status
  --------------- --------------- --------------- ----- -----------
  10.10.1.1       255.255.255.255 10.100.1.1        1    up
                                  10.200.2.2        1    down

  10.20.2.2       255.255.255.255 10.233.3.3        1    up
  10.20.2.2       255.255.255.255 10.234.4.4        1    up
  10.20.2.2       255.255.255.255 10.235.5.5        1    up

ECMP health-check ping interval: 1
ECMP health-check retries number: 3
```

ECMP route information shows the status of each ECMP route configured on the switch.

/info/l3/hash

ECMP Hashing Result

```
Enter SIP address: 10.0.0.1
Enter DIP address (0 for SIP only): 10.0.0.2
Enter number of ECMP paths: 3
Source 10.0.0.1 will go through route number 3
```

ECMP hashing information shows the status of ECMP hashing.

/info/l3/igmp

IGMP Multicast Group Information Menu

```
[IGMP Multicast Menu]
     querier  - Show IGMP Querier information
     mrouter  - Show IGMP Snooping Multicast Router Port information
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP group address
     dump     - Show all groups
     ipmcgrp  - Show all ipmc groups
```

Table 51 describes the commands used to display information about IGMP groups learned by the switch.

Table 51. IGMP Multicast Group Information Menu Options (/info/l3/igmp)

Command Syntax and Usage
`querier` Displays IGMP Querier information. For details, see page 78.
`mrouter` Displays IGMP Multicast Router menu. To view menu options, see page 78.
`find` *<IP address>* Displays a single IGMP multicast group by its IP address.
`vlan` *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.
`port` *<port number or alias>* Displays all IGMP multicast groups on a single port.
`trunk` *<trunk number>* Displays all IGMP multicast groups on a single trunk group.
`detail` *<IP address>* Displays details about IGMP multicast groups, including source and timer information.
`dump` Displays information for all multicast groups. For details, see page 79
`ipmcgrp` *<VLAN number>* Displays all IP multicast groups on a single VLAN.

/info/l3/igmp/querier <*VLAN number*>

IGMP Querier Information

```
Current IGMP Querier information:
 IGMP Querier information for vlan 1:
 Other IGMP querier - none
 Switch-querier enabled, current state: Querier
 Switch-querier type: Ipv4, address 0.0.0.0,
 Switch-querier general query interval: 125 secs,
 Switch-querier max-response interval: 100 'tenths of secs',
 Switch-querier startup interval: 31 secs, count: 2
 Switch-querier robustness: 2
 IGMP configured version is v3
 IGMP Operating version is v3
```

IGMP Querier information includes:

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

/info/l3/igmp/mrouter

IGMP Multicast Router Port Information Menu

```
[IGMP Multicast Router Menu]
     static   - Show all static multicast router ports installed
     dynamic  - Show all dynamic multicast router ports installed
     vlan     - Show all multicast router ports on a single vlan
     port     - Show all multicast router ports on a single port
     trunk    - Show all multicast router ports on a single trunk
     dump     - Show all learned multicast router ports
```

Table 52 describes the commands used to display information about multicast routers (Mrouters) learned through IGMP Snooping.

Table 52. IGMP Mrouter Information Menu Options (/info/igmp/mrouter)

Command Syntax and Usage
`static` Displays the static multicast router ports configured on the switch.
`dynamic` Displays the dynamic multicast router ports learned by the switch.

Table 52. IGMP Mrouter Information Menu Options (/info/igmp/mrouter)

Command Syntax and Usage
`vlan` *<VLAN number>* Displays the multicast router ports configured or learned on the selected VLAN.
`port` *<port no./alias>* Displays the multicast router ports configured or learned on the specified physical port.
`trunk` *<1-128>* Displays the multicast router ports configured or learned on the specified trunk.
`dump` Displays information for all multicast groups learned by the switch.

/info/l3/igmp/mrouter/dump
IGMP Multicast Router Dump Information

```
SrcIP              VLAN    Port       Version   Expires   MRT       QRV   QQIC

------------------ ------- -------    --------- --------  -------   ----  ----
10.1.1.1            2       21         V3        4:09     128        2     125
10.1.1.5            2       23         V2        4:09     125        -       -
10.10.10.43         9       24         V2          -        -        -       -
```

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)

/info/l3/igmp/dump
IGMP Group Information

```
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      EXT4    V3       INC    4:16    Yes
 10.1.1.5       232.1.1.1        2      EXT4    V3       INC    4:16    Yes
    *           232.1.1.1        2      EXT4    V3       INC     -      No
 10.10.10.43    235.0.0.1        9      EXT1    V3       INC    2:26    Yes
    *           236.0.0.1        9      EXT1    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

/info/l3/igmp/ipmcgrp
IPMC Group Information

```
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:

- IGMP source address
- IGMP Group address
- VLAN and port
- Type of IPMC group
- Expiration timer value

/info/l3/mld

MLD Information Menu

```
[MLD info Menu]
     mrouter  - Show MLD Multicast Router Port information
     groups   - Show all groups
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     if       - Show interface(s) mld information
     dump     - Show mld information
```

Table 53 describes the MLD information menu options.

Table 53. MLD Information Menu Options (/info/l3/mld)

Command Syntax and Usage
`mrouter` Displays MLD Mrouter information menu. To view menu options, see page 82.
`groups` Displays all MLD groups.
`find` *<IP6 address>* Displays a single MLD group by its IP address.
`vlan` *<VLAN number>* Displays all MLD groups on a single VLAN.
`port` *<port number>* Displays all MLD groups on a single port.
`trunk` *<trunk group number>* Displays all MLD groups on a single trunk group.
`if` *<interface number or a range of interface numbers>* Displays all MLD groups on the interface(s).
`dump` Displays information for all MLD groups.

/info/l3/mld/mrouter

MLD Mrouter Information Menu

```
[MLD Multicast Router Menu]
     dump  - Show all MLD multicast router ports
```

Table 54 describes the commands used to display information about MLD Mrouter ports.

Table 54. MLD Mrouter Information Menu Options (/info/l3/mld/mrouter)

Command Syntax and Usage
dump Displays information for MLD Mrouter ports. See page 82 for sample output.

/info/l3/mld/mrouter/dump

MLD Mrouter Dump Information

```
Source: fe80:0:0:0:200:bff:fe88:2748
Port/Vlan: XGE2/4
Interface: 3
QRV: 2  QQIC:125
Maximum Response Delay: 1000
Version: MLDv2 Expires:1:03
```

Table 55 describes the MLD Mrouter dump information displayed in the output.

Table 55. MLD Mrouter Dump Information (/info/l3/mld/mrouter/dump)

Statistic	Description
Source	Displays the link-local address of the reporter.
Port/Vlan	Displays the port/vlan on which the general query is received.
Interface	Displays the interface number on which the general query is received.
QRV	Displays the Querier's robustness variable value.
QQIC	Displays the Querier's query interval code.
Maximum Response Delay	Displays the configured maximum query response time.
Version	Displays the MLD version configured on the interface.
Expires	Displays the interval after which the multicast router decides that there are no more listeners for a multicast address or a particular source on a link.

/info/l3/vrrp

VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on the CN4093 provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

```
VRRP information:
  1: vrid 2, 205.178.18.210, if  1, renter, prio 100, master
  2: vrid 1, 205.178.18.202, if  1, renter, prio 100, backup
  3: vrid 3, 205.178.18.204, if  1, renter, prio 100, master
```

When virtual routers are configured, you can view the status of each virtual router using this command. VRRP information includes:

- Virtual router number
- Virtual router ID and IP address
- Interface number
- Ownership status
  - `owner` identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.
  - `renter` identifies virtual routers which are not owned by this device.
- Priority value. During the election process, the virtual router with the highest priority becomes master.
- Activity status
  - `master` identifies the elected master virtual router.
  - `backup` identifies that the virtual router is in backup mode.
  - `init` identifies that the virtual router is waiting for a startup event. For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.

/info/l3/if

Interface Information

```
Interface information:
126: IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::a17:f4ff:fe0a:1ef
127: IP4 10.43.98.33      255.255.255.0   9.43.98.255,     vlan 4095, up
128: IP4 10.43.95.162     255.255.255.0   9.43.95.255,     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)

/info/l3/ip6pmtu [<*destination IPv6 address*>]

IPv6 Path MTU Information

```
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.

/info/l3/ip

IP Information

```
IP information:
  AS number 0

Interface information:
126: IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::200:ff:fe00:ef
128: IP4 9.43.95.121     255.255.255.0   9.43.95.255,     vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
  4: 9.43.95.254,     FAILED

Default IP6 gateway information:

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


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


Current network filter settings:
  none

Current route map settings:
RIP is disabled.


OSPF is disabled.

OSPFv3 is disabled.

BGP is disabled.
```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Loopback interface information, if applicable
- 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

/info/l3/ikev2
IKEv2 Information

```
[IKEv2 Information Menu]
     info     - Show IKEv2 information
     cacert   - Show CA certificate information
     hcert    - Show host certificate information
```

Table 56 describes the commands used to display information about IKEv2.

Table 56. IKEv2 Information Menu Options (/info/l3/ikev2)

Command Syntax and Usage
`info` Displays all IKEv2 information. See page 86 for sample output.
`cacert` Displays CA certificate information.
`hcert` Displays host certificate information.

/info/l3/ikev2/info
IKEv2 Information Dump

```
IKEv2 retransmit time:       20

IKEv2 cookie notification:   disable

IKEv2 authentication method: Pre-shared key

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

Local preshare key:          ibm123

IKEv2 choose IPv6 address as ID type
No SAD entries.
```

IKEv2 information includes:

- IKEv2 retransmit time, in seconds.
- Whether IKEv2 cookie notification is enabled.
- The IKEv2 proposal in force. This includes the encryption algorithm (cipher), the authentication algorithm type, and the Diffie-Hellman (DH) group, which determines the strength of the key used in the key exchange process. Higher DH group numbers are more secure but require additional time to compute the key.
- The local preshare key.
- Whether IKEv2 is using IPv4 or IPv6 addresses as the ID type.
- Security Association Database (SAD) entries, if applicable.

/info/l3/ipsec

IPsec Information Menu

```
[IPsec Information Menu]
     sa       - Show all sa information
     spd      - Show all spd information
     dpolicy  - Show dynamic policy information
     mpolicy  - Show manual policy information
     txform   - Show ipsec transform information
     selector - Show ipsec traffic selector information
```

Table 57 describes the commands used to display information about IPsec.

Table 57. IPsec Information Menu Options (/info/l3/ipsec)

Command Syntax and Usage
`sa` Displays all security association information.
`spd` Displays all security policy information.
`dpolicy` *<1-10>* Displays dynamic policy information.
`mpolicy` *<1-10>* Displays manual policy information. See page 87 for sample output.
`txform` *<1-10>* Displays IPsec transform information.
`selector` *<1-10>* Displays IPsec traffic selector information.

/info/l3/ipsec/mpolicy

IPsec Manual Policy Information

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

IPsec manual policy information includes:

- The IP address of the remote peer
- The transform set ID associated with this policy

- Traffic selector ID associated with this policy
- ESP inbound SPI
- ESP inbound encryption key
- ESP inbound authentication key
- ESP outbound SPI
- ESP outbound encryption key
- ESP outbound authentication key
- The interface to which this manual policy has been applied

/info/qos

Quality of Service Information Menu

```
[QoS Menu]
     8021p    - Show QOS 802.1p information
     rdetect  - Show QOS WRED ECN information
```

Table 58. QoS Menu Options (/info/qos)

Command Syntax and Usage
8021p Displays 802.1p Information. For details, see page 88.
rdetect Displays WRED ECN information. For details, see page 90.

/info/qos/8021p

802.1p Information

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

Current port priority information:
Port   Priority  COSq  Weight
-----  --------  ----  ------
INTA1       0       0      1
INTA2       0       0      1
...
MGT1        0       0      1
EXT1        0       0      1
EXT2        0       0      1
EXT3        0       0      1
EXT4        0       0      1
...
```

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

Table 59. 802.1p Priority-to-COS Queue Parameter Descriptions

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

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

Table 60. 802.1p Port Priority Parameter Descriptions

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

/info/qos/rdetect

WRED and ECN Information

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

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

/info/acl

Access Control List Information Menu

```
[ACL Information Menu]
     acl-list  - Show ACL list
     acl-list6 - Show IPv6 ACL list
     acl-grp   - Show ACL group     vmap      - Show VMAP
```

Table 61. ACL Information Menu Options (/info/acl)

Command Syntax and Usage
`acl-list` *<ACL number>* Displays ACL list information. For details, see page 90.
`acl-list6` *<ACL number>* Displays IPv6 ACL list information.
`acl-grp` *<ACL group number>* Displays ACL group information.
`vmap` *<VMAP number>* Displays VMAP list information.

/info/acl/acl-list

Access Control List Information

```
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 list.

Table 62. ACL List 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).

/info/rmon

RMON Information Menu

```
[RMON Information Menu]
     hist    - Show RMON History group information
     alarm   - Show RMON Alarm group information
     event   - Show RMON Event group information
     dump    - Show all RMON information
```

The following table describes the Remote Monitoring (RMON) Information menu options.

Table 63. RMON Information Menu Options (/info/rmon)

Command Syntax and Usage
`hist` Displays RMON History information. For details, see page 92.
`alarm` Displays RMON Alarm information. For details, see page 93.
`event` Displays RMON Event information. For details, see page 94.
`dump` Displays all RMON information.

/info/rmon/hist

RMON History Information

```
RMON History group configuration:

Index IFOID                          Interval Rbnum Gbnum
----- ------------------------------ -------- ----- -----
   1  1.3.6.1.2.1.2.2.1.1.24               30     5     5
   2  1.3.6.1.2.1.2.2.1.1.22               30     5     5
   3  1.3.6.1.2.1.2.2.1.1.20               30     5     5
   4  1.3.6.1.2.1.2.2.1.1.19               30     5     5
   5  1.3.6.1.2.1.2.2.1.1.24             1800     5     5

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

The following table describes the RMON History Information parameters.

Table 64. RMON History Parameter Descriptions

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

/info/rmon/alarm

RMON Alarm Information

```
RMON Alarm group configuration:

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

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

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

The following table describes the RMON Alarm Information parameters.

Table 65. RMON Alarm Parameter Descriptions

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

Table 65. RMON Alarm Parameter Descriptions (continued)

Parameter	Description
OID	Displays the MIB Object Identifier for each alarm index.
Owner	Displays the owner of the alarm instance.

/info/rmon/event

RMON Event Information

```
RMON Event group configuration:

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

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

The following table describes the RMON Event Information parameters.

Table 66. RMON Event Parameter Descriptions

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

/info/link

Link Status Information

```
Alias   Port   Speed    Duplex     Flow Ctrl      Link       Name
------- ----   -----   --------  --TX-----RX--   ------     ------
INTA1   1      1G/10G    full     yes    yes      down       INTA1
INTA2   2      1G/10G    full     yes    yes      down       INTA2
INTA3   3      1G/10G    full     yes    yes      down       INTA3
INTA4   4      1G/10G    full     yes    yes      down       INTA4
...
INTA14  14     1G/10G    full     yes    yes      down       INTA14
INTB1   15     1G/10G    full     yes    yes      down       INTB1
INTB2   16     1G/10G    full     yes    yes      down       INTB2
INTB3   17     1G/10G    full     yes    yes      down       INTB3
INTB4   18     1G/10G    full     yes    yes      down       INTB4
...
INTC14  42     1G/10G    full     yes    yes      down       INTC14
EXT1    43     1G/10G    full      no     no      down       EXT1
EXT2    44     1G/10G    full      no     no      down       EXT2
EXT3    45     10000     full      no     no       up        EXT3
EXT4    46     1G/10G    full      no     no      down       EXT4
...
EXT20   62     10000     full      no     no    disabled     EXT20
EXT21   63     10000     full      no     no    disabled     EXT21
EXT22   64     10000     full      no     no    disabled     EXT22
EXTM    65      1000     full     yes    yes       up        EXTM
MGT1    66      1000     full      no     no       up        MGT1
```

Note: The sample screen might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex system chassis 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 a CN4093 slot, including:

- Port alias and number
- Port speed
- Duplex mode (half, full, any)
- Flow control for transmit and receive (no, yes, or both)
- Link status (up, down, or disabled)

/info/port

Port Information

```
Alias   Port Tag RMON Lrn Fld PVID       NAME                 VLAN(s)
------- ---- --- ---- --- --- ----- -------------- ------------------------------
INTA1   1     n   d    e   e     1  INTA1          1
INTA2   2     n   d    e   e     1  INTA2          1
INTA3   3     n   d    e   e     1  INTA3          1
INTA4   4     n   d    e   e     2  INTA4          2
INTA5   5     n   d    e   e     1  INTA5          1
INTA6   6     n   d    e   e     1  INTA6          1
INTA7   7     n   d    e   e     1  INTA7          1
INTA8   8     n   d    e   e     1  INTA8          1
INTA9   9     n   d    e   e     1  INTA9          1
INTA10  10    n   d    e   e     1  INTA10         1
INTA11  11    n   d    e   e     1  INTA11         1
INTA12  12    n   d    e   e     1  INTA12         1
INTA13  13    n   d    e   e     1  INTA13         1
INTA14  14    n   d    e   e     1  INTA14         1
INTB1   15    n   d    e   e     1  INTB1          1
INTB2   16    n   d    e   e     1  INTB2          1
...
INTC13  41    n   d    e   e     1  INTC13         1
INTC14  42    n   d    e   e     1  INTC14         1
EXT1    43    n   d    e   e     1  EXT1           1
EXT2    44    n   d    e   e     1  EXT2           1
EXT3    45    n   d    e   e   100  EXT3           100
EXT4    46    n   d    e   e     1  EXT4           1
...
EXT20   62    n   d    e   e     1  EXT20          1
EXT21   63    n   d    e   e     1  EXT21          1
EXT22   64    n   d    e   e     1  EXT22          1
EXTM    65    n   d    e   e  4095  EXTM           4095
MGT1    66    y   d    e   e  4095  MGT1           4095

* = PVID is tagged.
```

Note: The sample screens that appear in this document might differ slightly from the screens displayed by your system. Screen content varies based on the type of Flex System chassis 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`)
- Type of port (Internal, External, or Management)
- Whether the port has Remote Monitoring (RMON) enabled
- Whether the port has FDB learning enabled (`Lrn`)
- Whether the port has Port Flooding enabled (`Fld`)
- Port VLAN ID (`PVID`)
- Port name
- VLAN membership

/info/transcvr

Port Transceiver Status This command displays information about the

```
Name             TX  RXLos TXFlt Volts DegsC TXuW  RXuW  Media   Laser  Approval
---------------- --- ----- ----- ----- ----- ----- ----- ------- ------ --------
44 SFP+  2       < NO Device Installed >
45 SFP+  3       Ena LINK  no     3.29 29.5  556.9 580.5 SR SFP+ 850nm  Approved
         Blade Network    Part:BN-CKM-SP-SR     Date:110329 S/N:AA1113AG1B1
46 SFP+  4       < NO Device Installed >
47 SFP+  5       N/A LINK  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:080710 S/N:BNT0828075
48 SFP+  6       < NO Device Installed >
49 SFP+  7       N/A Down  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:080710 S/N:BNT08280W0
50 SFP+  8       < NO Device Installed >
51 SFP+  9       N/A Down  -N/A-  -.-- --.-  ---.- ---.- CU SFP  -N/A-  Approved
         Blade Network    Part:BN-CKM-S-T       Date:100717 S/N:BNT10288NM
52 SFP+ 10       < NO Device Installed >
...
57 Q10G 15.1     < NO Device Installed >
58 Q10G 15.2     < NO Device Installed >
59 Q10G 15.3     < NO Device Installed >
60 Q10G 15.4     < NO Device Installed >
61 Q10G 16.1     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
62 Q10G 16.2     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
63 Q10G 16.3     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
64 Q10G 16.4     N/A Down  -N/A-  -.-- --.-  ---.- ---.- 3m QDAC -N/A-  Accepted
         BLADE NETWORK    Part:BN-QS-QS-CBL-3M  Date:110422 S/N:3549Y350VT14K0HN
```

transceiver module on each port, as follows:

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

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

Table 67. 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.

/info/virt
Virtualization Information

```
[Virtualization Menu]
     vm        - Show Virtual Machine information
     vnic      - Show vNIC information
     evb       - Show Edge Virtual Bridge information
```

Table 68 describes general virtualization information options. More details are available in the following sections.

Table 68. Virtualization Information Options (/info/virt)

Command Syntax and Usage
`vm` Displays the Virtual Machines (VM) information menu. For details, see page 99.
`vnic` Displays the Virtual Network Interface Card (vNIC) information menu. For details, see page 99.
`evb` Displays the Edge Virtual Bridge (EVB) information menu. For details, see page 102.

/info/virt/vm
Virtual Machines Information

```
[Virtual Machine Menu]
     vmware   - Show VMware-specific information
     port     - Show per port Virtual Machine information
     trunk    - Show per trunk Virtual Machine information
     dump     - Show all the Virtual Machine information
```

Table 69. Virtual Machines (VM) Information Options (/info/virt/vm)

Command Syntax and Usage
`vmware` Displays the VMware-specific information menu.
`port` Displays Virtual Machine information for the selected port.
`trunk` Displays Virtual Machine information for the selected trunk.
`dump` Displays all Virtual Machine information. For details, see page 99.

/info/virt/vm/dump
Virtual Machine (VM) Information

```
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

/info/virt/vm/vmware

VMware Information

```
[VMware-specific Information Menu]
   hosts    - Show the names of all VMware Hosts in Data Center
   showhost - Show networking information for the specified VMware Host
   showvm   - Show networking information for the specified VMware VM
   vms      - Show the names of all VMware VMs in the Data Center
```

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 70. VMware Information Options (/info/virt/vm/vmware)

Command Syntax and Usage
`hosts` Displays a list of VMware hosts. For details, see page 100.
`showhost` *<host UUID> | <host IP address> | <host host name>* Displays detailed information about a specific VMware host.
`showvm` *<VM UUID> | <VM IP address> | <VM name>* Displays detailed information about a specific Virtual Machine (VM).
`vms` Displays a list of VMs.

/info/virt/vm/vmware/hosts

VMware Host Information

```
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.

/info/virt/vnic

Virtual Network Interface Card Information

```
[vNIC Information Menu]
     vnic     - Show vNIC Information
     vnicgrp  - Show vNIC Group Information
     dump     - Show vNIC and vNIC Group Information
```

Table 71. Virtual Network Interface Card (vNIC) Information Options (/info/virt/vnic)

Command Syntax and Usage
`vnic` Displays vNIC information. For details, see page 101.
`vnicgrp` Displays information about each vNIC Group, including: – Status (enabled or disabled) – VLAN assigned to the vNIC Group – Uplink Failover status (enabled or disabled) – Link status for each vNIC (up, down, or disabled) – Port link status for each port associated with the vNIC Group (up, down, or disabled) For details, see page 102.
`dump` Displays vnic and vnic group information.

/info/virt/vnic/vnic
Virtual NIC (vNIC) Information

```
vNIC      vNICGroup  Vlan    MaxBandwidth  Type    MACAddress          Link
--------  ---------  ------  ------------  ------- ------------------  ---------
INTA1.1    1            101            25   Default  00:00:c9:5b:b7:d0   up
INTA2.2    2            102            10   Default  00:00:c9:5b:cf:d1   down
INTB1.2   12            202            25   Default  00:00:c9:5b:b7:c9   up
INTB9.4    #              *            25   Default           none       disabled

# = Not added to any vNIC group
* = Not added to any vNIC group or no vlan set for its vNIC group
```

vNIC information includes the following for each vNIC:

- vNIC ID
- vNIC Group that contains the vNIC
- VLAN assigned to the vNIC Group
- Maximum bandwidth allocated to the vNIC
- MAC address of the vNIC, if applicable
- Link status (up, down, or disabled)

/info/virt/vnic/vnicgrp

vNIC Group Information

```
vNIC Group  1: enabled
-------------------------------------------------------------------
VLAN         : 101
Failover     : disabled

vNIC        Link
----------  ---------
INTA9.1     up
INTA10.1    up
INTB10.2    down

Port        Link
----------  ---------
INTA11    up

UplinkPort  Link
----------  ---------
EXT6        up
```

vNIC Group information includes the following for each vNIC Group:

- Status (enabled or disabled)
- VLAN assigned to the vNIC Group
- Uplink Failover status (enabled or disabled)
- Link status for each vNIC (up, down, or disabled)
- Port link status for each port associated with the vNIC Group (up, down, or disabled)

/info/virt/evb

EVB Information

```
[EVB Information Menu]
     vdp      - Show Virtual Station Interface information
```

Table 72 describes the Edge Virtual Bridge (EVB) information options.

Table 72. EVB Information Options

Command Syntax and Usage
vdp Displays the Virtual Station Interface information menu. For details, see page 103.

/info/virt/evb/vdp

VSI Information

```
[VSI Information Menu]
     vms       - Show all active VMs
     tlvs      - Show all active VDP tlvs
     vsidb     - Show VSI DataBase information
```

Table 73 describes the Virtual Station Interface (VSI) information options.

Table 73. VSI Information Options

Command Syntax and Usage
vms Displays all active Virtual Machines (VMs).
tlvs Displays all active Virtual Station Interface (VSI) Discovery and Configuration Protocol (VDP) type-length-values (TLVs).
vsidb Displays Virtual Station Interface database information.

/info/cee

Converged Enhanced Ethernet Information

```
[CEE Information Menu]
    dcbx      - DCB Capability Exchange Protocol (DCBX) Information Menu
    ets       - Enhanced Transmission Selection Information Menu
    pfc       - Priority Flow Control Information Menu
    dump      - Show all CEE information
```

Table 74 describes the Converged Enhanced Ethernet (CEE) information options.

Table 74. CEE Information Options (/info/cee)

Command Syntax and Usage
dcbx Displays the DCB Capability Exchange Protocol (DCBX) information menu. To view the menu options, see page 104.
ets Displays the Enhanced Transmission Selection (ETS) information menu. To view the menu options, see page 109.
pfc Displays the Priority Flow Control (PFC) information menu. To view the menu options, see page 110.
dump Displays all CEE information.

/info/cee/dcbx
DCBX Information

```
[DCBX Information Menu]
    ctrl     - Show DCBX Control state machine information
    feat     - Show DCBX Feature state machine information
    ets      - Show DCBX ETS state machine information
    pfc      - Show DCBX PFC state machine information
    app      - Show DCBX Application Protocol state machine information
    dump     - Show all DCBX information
```

Table 75 describes the Data Center Bridging Capability Exchange (DCBX) protocol information options.

Table 75. DCBX Information Options (/info/cee/dcbx)

Command Syntax and Usage
`ctrl` [<*port alias or number*>] Displays information about the DCBX Control state machine. For details, see page 104.
`feat` [<*port alias or number*>] Displays information about the DCBX Feature state machine. For details, see page 105.
`ets` [<*port alias or number*>] Displays information about the DCBX ETS state machine. For details, see page 106.
`pfc` [<*port alias or number*>] Displays information about the DCBX PFC state machine. For details, see page 107.
`app` [<*port alias or number*>] Displays information about the DCBX Application Protocol state machine on the selected port. For details, see page 108.
`dump` [<*port alias or number*>] Displays all DCBX information, globally or only for a selected port.

/info/cee/dcbx/ctrl [<*port alias or number*>]
DCBX Control Information

```
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

/info/cee/dcbx/feat [<*port alias or number*>]

DCBX Feature Information

```
DCBX Port Feature State-machine Info
====================================
Alias Port Type    AdmState Will Advrt OpVer MxVer PrWill SeqNo Err OperMode Syncd
----- ---- ------- -------- ---- ----- ----- ----- ------ ----- --- -------- ---
INTA1  1   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
INTA2  2   ETS     enabled  No   Yes   0     0     Yes    4     No  enabled  Yes
INTA3  3   ETS     enabled  No   Yes   0     0     No     0     No  disabled No
INTA4  4   ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA5  5   ETS     enabled  No   Yes   0     0     Yes    1     No  enabled  Yes
INTA6  6   ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA7  7   ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA8  8   ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA9  9   ETS     disabled No   Yes   0     0     No     0     No  disabled No
INTA10 10  ETS     enabled  No   Yes   0     0     No     0     No  disabled No
...
```

The following table describes the DCBX Feature information.

Table 76. 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.

Table 76. DCBX Feature Information Fields

Parameter	Description
OperMode	Operating status negotiated with the peer device (enabled or disabled)
Syncd	Synchronization status between this port and the peer (Yes or No)

/info/cee/dcbx/ets [<*port alias or number*>]

DCBX ETS Information

```
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   PGID0    PGID0
INTA2 2    4        PGID2   PGID0    PGID0
INTA2 2    5        PGID2   PGID0    PGID0
INTA2 2    6        PGID2   PGID0    PGID0
INTA2 2    7        PGID2   PGID0    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 77. 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

Table 77. DCBX Feature Information Fields

Parameter	Description
BwOper	Bandwidth allocation negotiated with the peer (operating bandwidth)
BwPeer	Bandwidth allocation configured on the peer

/info/cee/dcbx/pfc [<*port alias or number*>]

DCBX PFC Information

```
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    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
```

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

/info/cee/dcbx/app [<*port alias or number*>]

DCBX Application Protocol Information

```
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        enabled    enabled    enabled
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

FIP Snooping Priority Information
=================================
Protocol ID               : 0x8914
Selector Field            : 0
Organizationally Unique ID: 0x1b21

Alias Port Priority EnableDesr EnableOper EnablePeer
----- ---- -------- ---------- ---------- ----------
INTA2 2    0        enabled    enabled    enabled
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
```

The following table describes the DCBX Application Protocol information.

Table 78. 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
Alias	Port alias
Port	Port number
Priority	802.1p value

Table 78. DCBX Application Protocol Information Fields

Parameter	Description
EnableDesr	Status configured on this switch
EnableOper	Status negotiated with the peer (operating status)
EnablePeer	Status configured on the peer

/info/cee/ets
ETS Information Menu

```
[ETS Information Menu]
     dump     - Show all ETS information
```

Table 79 describes the Enhanced Transmission Selection (ETS) information options.

Table 79. ETS Information Options (/info/cee/ets)

Command Syntax and Usage
dump Displays global ETS information. For details, see page 109.

/info/cee/ets/dump
ETS Information

```
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

/info/cee/pfc
PFC Information Menu

```
[PFC Information Menu]
     port     - Show PFC information related to a port
     dump     - Show all PFC information
```

Table 80 describes the Priority Flow Control (PFC) information options.

Table 80. PFC Information Options (/info/cee/pfc)

Command Syntax and Usage
`port` *<port alias or number>* Displays PFC information for the selected port.
`dump` Displays PFC information for all ports.

/info/cee/pfc/dump

PFC Information

```
PFC information for Port INT1:

PFC - ON

Priority   State   Description
--------   -----   -----------
   0        Dis
   1        Dis
   2        Dis
   3        Ena
   4        Dis
   5        Dis
   6        Dis
   7        Dis
```

/info/fcoe

FCoE Information

```
[Fibre Channel over Ethernet Information Menu]
     fips     - FIP Snooping Information Menu
     dump     - Show all FCOE information
```

Table 81 describes the Fiber Channel over Ethernet (FCoE) information options.

Table 81. FCoE Information Options (/info/fcoe)

Command Syntax and Usage
`fips` Displays the FIP Snooping information menu.
`dump` Displays all current FCoE information.

/info/fcoe/fips
FIP Snooping Information

```
[FIP Snooping Information Menu]
     port      - Show FIP snooping ACLs installed on a port
     fcf       - Show all FCF detected
     fcoe      - Show all FCOE connections detected
     dump      - Show all FIP snooping ACLs that are installed
```

Table 82 describes the Fiber Channel Initialization Protocol (FIP) Snooping information options.

Table 82. FIP Snooping Information Options (/info/fcoe/fips)

Command Syntax and Usage
`port` *<port alias or number>* Displays FIP Snooping (FIPS) information for the selected port, including a list of current FIPS ACLs. For details, see page 112.
`fcf` Displays FCF information for all ports.
`fcoe` Displays FCoE connections established on the switch.
`dump` Displays FIP Snooping information for all ports.

/info/fcoe/fips/port *<port alias or number>*
FIP Snooping Port Information

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

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

FIP Snooping port information includes the following:

- Fiber Channel Forwarding (FCF) mode

- Number of FCF links connected to the port
- List of FIP Snooping ACLs assigned to the port

/info/dump

Information Dump

Use the dump command to dump all switch information available from the Information Menu (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 4. The Statistics Menu

You can 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.

/stats

Statistics Menu

```
[Statistics Menu]
     port     - Port Stats Menu
     trunk    - Trunk Group Stats Menu
     l2       - Layer 2 Stats Menu
     l3       - Layer 3 Stats Menu
     mp       - MP-specific Stats Menu
     acl      - ACL Stats Menu
     fcoe     - FCOE Stats Menu
     snmp     - Show SNMP stats
     ntp      - Show NTP stats
     clrmp    - Clear all MP related stats
     clrcpu   - Clear CPU utilization
     clrports - Clear stats for all ports
     dump     - Dump all stats
```

The information provided by each menu option is briefly described in Table 83, with pointers to detailed information.

Table 83. Statistics Menu Options (/stats)

Command Syntax and Usage
`port` *<port alias or number>* Displays the Port Statistics Menu for the specified port. Use this command to display traffic statistics on a port-by-port basis. Traffic statistics are included in SNMP Management Information Base (MIB) objects. To view menu options, see page 117.
`trunk` *<trunk group number>* Displays the Trunk Statistics Menu for the specified port. To view menu options, see page 133.
`l2` Displays the Layer 2 Statistics Menu. To view menu options, see page 134.
`l3` Displays the Layer 3 Stats Menu. To view menu options, see page 141.
`mp` Displays the Management Processor Statistics Menu. Use this command to view information on how switch management processes and resources are currently being allocated. To view menu options, see page 173.
`acl` Displays ACL Statistics menu. To view menu options, see page 186.

Table 83. Statistics Menu Options (/stats)

Command Syntax and Usage
`fcoe [clear]` Displays Fiber Channel over Ethernet (FCoE) Statistics. To view details, see page 187. You can use the `clear` option to delete all FCoE statistics.
`snmp` Displays SNMP statistics. See page 188 for sample output.
`ntp [clear]` Displays Network Time Protocol (NTP) Statistics. See page 191 for a sample output and a description of NTP Statistics. You can use the `clear` option to delete all NTP statistics.
`clrmp` Clears all management processor statistics.
`clrcpu` Clears all CPU use statistics.
`clrports` Clears statistics counters for all ports.
`dump` Dumps all switch statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command. For details, see page 192.

/stats/port <*port alias or number*>
Port Statistics Menu

This menu displays traffic statistics on a port-by-port basis. Traffic statistics include SNMP Management Information Base (MIB) objects.

```
[Port Statistics Menu]
     8021x    - Show 802.1x stats
     bootp    - Show BOOTP relay stats
     brate    - Show interface bitrate[Kbps] usage (continuos)
     brg      - Show bridging ("dot1") stats
     brg-rate - Show bridging ("dot1") stats/second
     ether    - Show Ethernet ("dot3") stats
     eth-rate - Show Ethernet ("dot3") stats/second
     qos-cnt  - Show QoS Queues Counters
     qos-rate - Show QoS Queues Rate
     if       - Show interface ("if") stats
     if-rate  - Show interface ("if") stats/second
     ip       - Show Internet Protocol ("IP") stats
     ip-rate  - Show Internet Protocol ("IP") stats/second
     link     - Show link stats
     maint    - Show port maintenance stats
     rmon     - Show RMON stats
     dump     - Show all port stats
     clear    - Clear all port stats
```

Table 84. Port Statistics Menu Options (/stats/port)

Command Syntax and Usage
`8021x` Displays IEEE 802.1x statistics for the port. See page 119 for sample output.
`bootp` Displays BOOTP Relay statistics for the port. See page 122 for sample output.
`brate` Displays continuous interface bitrate usage in Kb per second.
`brg` Displays bridging (“dot1”) statistics for the port. See page 122 for sample output.
`brg-rate` Displays bridging (“dot1”) statistics per second for the port.
`ether` Displays Ethernet (“dot3”) statistics for the port. See page 123 for sample output.
`ether-rate` Displays Ethernet (“dot3”) statistics per second for the port.
`qos-cnt` Displays the total number of packets and bytes either successfully transmitted or dropped for each queue of the port. See page 126 for sample output.

Table 84. Port Statistics Menu Options (/stats/port) (continued)

Command Syntax and Usage
`qos-rate` Displays the number of packets and bytes per second either successfully transmitted or dropped for each queue of the port. See page 127 for sample output.
`if` Displays interface statistics for the port. See page 128 for sample output.
`if-rate` Displays interface statistics per second for the port.
`ip` Displays IP statistics for the port. See page 130 for sample output.
`ip-rate` Displays IP statistics per second for the port.
`link` Displays link statistics for the port. See page 131 for sample output.
`maint` Displays detailed maintenance statistics for the port.
`rmon` Displays Remote Monitoring (RMON) statistics for the port. See page 131 for sample output.
`dump` This command dumps all statistics for the selected port.
`clear` This command clears all the statistics on the selected port.

/stats/port <*port alias or number*>/8021x

802.1x Authenticator Statistics

This menu option enables you to display the 802.1x authenticator statistics of the selected port.

```
Authenticator Statistics:
  eapolFramesRx          = 925
  eapolFramesTx          = 3201
  eapolStartFramesRx     = 2
  eapolLogoffFramesRx    = 0
  eapolRespIdFramesRx    = 463
  eapolRespFramesRx      = 460
  eapolReqIdFramesTx     = 1820
  eapolReqFramesTx       = 1381
  invalidEapolFramesRx   = 0
  eapLengthErrorFramesRx = 0
  lastEapolFrameVersion  = 1
  lastEapolFrameSource   = 00:01:02:45:ac:51
```

Table 85. 802.1x Authenticator Statistics of a Port (/stats/port/8021x)

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

/stats/port <*port alias or number*>/8021x

802.1x Authenticator Diagnostics

This menu option enables you to display the 802.1x authenticator diagnostics of the selected port.

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

Table 86. 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authEntersConnecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhile Connecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEnters Authenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
authSuccessesWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
authTimeoutsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.

Table 86. 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
authReauthsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhile Authenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccess Challenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
backendOtherRequests ToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNak ResponsesFrom Supplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator.s chosen EAP-method.

Table 86. 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

/stats/port <*port alias or number*>/bootp
BOOTP Relay Statistics

This menu option enables you to display the BOOTP Relay statistics of the selected port.

```
BOOTP Relay statistics for port EXT1:

Requests received from client:        0
Requests relayed to server:           0
Requests relayed with option 82:      0
Requests dropped due to ...
  - relay not allowed:                0
  - no server or unreachable server:  0
  - packet or processing errors:      0
Replies received from server:         0
Replies relayed to client:            0
Replies dropped due to ...
  - packet or processing errors:      0
```

/stats/port <*port alias or number*>/brg
Bridging Statistics

This menu option enables you to display the bridging statistics of the selected port.

```
Bridging statistics for port INTA1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 87. Bridging Statistics of a Port (/stats/port/brg)

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.

/stats/port <*port alias or number*>/ether
Ethernet Statistics

This menu option enables you to display the bridging statistics of the selected port.

```
Ethernet statistics for port INTA1:
dot3StatsAlignmentErrors:                NA
dot3StatsFCSErrors:                       0
dot3StatsSingleCollisionFrames:           0
dot3StatsMultipleCollisionFrames:         0
dot3StatsLateCollisions:                  0
dot3StatsExcessiveCollisions:             0
dot3StatsInternalMacTransmitErrors:       0
dot3StatsFrameTooLongs:                   0
dot3StatsInternalMacReceiveErrors:        0
```

Table 88. Ethernet Statistics of a Port

Statistics	Description
dot3StatsAlignmentErrors	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.
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
dot3StatsMultipleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.

Table 88. Ethernet Statistics of a Port (continued)

Statistics	Description
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.
dot3StatsFrameToo Longs	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.

/stats/port <*port alias or number*>/qos-cnt

QoS Queue Counter-Based Statistics

This option displays the counter-based QoS queue statistics of the selected port

```
QoS statistics for port INTA14:
QoS Queue 0:
    Tx Packets:                          664872
    Dropped Packets:                          0
    Tx Bytes:                          46791050
    Dropped Bytes:                            0
QoS Queue 1:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 2:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 3:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 4:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 5:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 6:
    Tx Packets:                               0
    Dropped Packets:                          0
    Tx Bytes:                                 0
    Dropped Bytes:                            0
QoS Queue 7:
    Tx Packets:                            9112
    Dropped Packets:                          0
    Tx Bytes:                           1463040
    Dropped Bytes:                            0
```

Table 89. QoS Queue Counter-Based Statistics of a Port

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

/stats/port <*port alias or number*>/qos-rate

QoS Queue Rate-Based Statistics

This option displays the rate-based QoS queue statistics of the selected port

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

Table 90. QoS Queue Rate-Based Statistics of a Port

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

/stats/port <*port alias or number*>/if
Interface Statistics

This menu option enables you to display the interface statistics of the selected port.

```
Interface statistics for port EXT1:
                     ifHCIn Counters       ifHCOut Counters
Octets:                  51697080313            51721056808
UcastPkts:                  65356399               65385714
BroadcastPkts:                     0                   6516
MulticastPkts:                     0                      0
FlowCtrlPkts:                      0                      0
Discards:                          0                      0
Errors:                            0                  21187

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:                    0
```

Table 91. Interface Statistics of a Port (/stats/port/if)

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 91. Interface Statistics of a Port (/stats/port/if)

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

Table 91. Interface Statistics of a Port (/stats/port/if)

Statistics	Description
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	HOL-blocking Discards = Discarded because of Head Of Line (HOL) blocking mechanism. Low priority packets are placed in a separate queue and can be discarded as applications or the TCP protocol keep track of whether a retransmission is necessary or not. HOL blocking is necessary to wait until an overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of Memory Management Unit.
Other Discards	Discarded packets not included in any category.

/stats/port <*port alias or number*>/ip
Interface Protocol Statistics

This menu option enables you to display the interface statistics of the selected port.

```
GEA IP statistics for port INTA1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 92. Interface Protocol Statistics of a Port (/stats/port/ip)

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.

/stats/port <*port alias or number*>/link
Link Statistics

This menu enables you to display the link statistics of the selected port.

```
Link statistics for port INTA1:
linkStateChange:            1
```

Table 93. Link Statistics of a Port (/stats/port/link)

Statistics	Description
linkStateChange	The total number of link state changes.

/stats/port <*port alias or number*>/rmon
RMON Statistics

This menu enables you to display the Remote Monitoring (RMON) statistics of the selected port.

```
RMON statistics for port EXT2:

etherStatsDropEvents:               NA
etherStatsOctets:                    0
etherStatsPkts:                      0
etherStatsBroadcastPkts:             0
etherStatsMulticastPkts:             0
etherStatsCRCAlignErrors:            0
etherStatsUndersizePkts:             0
etherStatsOversizePkts:              0
etherStatsFragments:                NA
etherStatsJabbers:                   0
etherStatsCollisions:                0
etherStatsPkts64Octets:              0
etherStatsPkts65to127Octets:         0
etherStatsPkts128to255Octets:        0
etherStatsPkts256to511Octets:        0
etherStatsPkts512to1023Octets:       0
etherStatsPkts1024to1518Octets:      0
```

Table 94. RMON Statistics of a Port (/stats/port/rmon)

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

Table 94. RMON Statistics of a Port (/stats/port/rmon)

Statistics	Description
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsCRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).

Table 94. RMON Statistics of a Port (/stats/port/rmon)

Statistics	Description
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

/stats/trunk <*trunk group number*>
Trunk Statistics Menu

This menu allows you to display traffic statistics for the selected trunk group.

```
[Trunk Group Statistics Menu]
     if       - Show interface ("if") stats
     clear    - Clear all trunk group stats
```

Table 95. Trunk Statistics Menu Options (/stats/trunk)

Command Syntax and Usage
`if` Displays interface statistics for the trunk group.
`clear` This command clears all the statistics on the selected trunk group.

/stats/l2

Layer 2 Statistics Menu

```
[Layer 2 Statistics Menu]
     fdb      - Show FDB stats
     lacp     - Show LACP stats
     hotlink  - Show Hot Links stats
     lldp     - Show LLDP port stats
     oam      - Show OAM stats
     vlag     - Show vLAG stats
```

The Layer 2 statistics provided by each menu option are briefly described in Table 96, with pointers to detailed information.

Table 96. Layer 2 Statistics Menu Options (/stats/l2)

Command Syntax and Usage
`fdb [clear]` Displays FDB statistics. See page 135 for sample output. Use the `clear` option to delete all FDB statistics.
`lacp [`*<port alias or number>*`|clear]` Displays Link Aggregation Control Protocol (LACP) statistics for a specified port, or for all ports if no port is specified. See page 135 for sample output. Use the `clear` option to delete all LACP statistics.
`hotlink` Displays Hotlinks statistics. See page 136 for sample output.
`lldp [`*<port alias or number>*`|clear]` Displays LLDP statistics for a specified port, or for all ports if no port is specified. See page 137 for sample output. Use the `clear` option to delete all LLDP statistics.
`oam` Displays the OAM Statistics menu. See page 137 for sample output.
`vlag` Displays vLAG Statistics menu. See page 138 for sample output.

/stats/l2/fdb [clear]

FDB Statistics

```
FDB statistics:
 current:           83   hiwat:             855
```

This menu option enables you to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches.

FDB statistics are described in the following table:

Table 97. Forwarding Database Statistics (/stats/fdb)

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

Use the `clear` option to delete all FDB statistics.

/stats/l2/lacp [<*port alias or number*>|clear]

LACP Statistics

```
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 98. LACP Statistics (/stats/l2/lacp)

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.

Table 98. LACP Statistics (/stats/l2/lacp)

Statistic	Description
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.

Use the `clear` option to delete all LACP statistics.

/stats/l2/hotlink
Hotlinks Statistics

```
Hot Links Trigger Stats:

Trigger 1 statistics:
    Trigger Name: Trigger 1
    Master active:          0
    Backup active:          0
    FDB update:             0   failed: 0
```

The following table describes the Hotlinks statistics:

Table 99. Hotlinks Statistics (/stats/l2/hotlink)

Statistic	Description
Master active	Total number of times the Master interface transitioned to the Active state.
Backup active	Total number of times the Backup interface transitioned to the Active state.
FDB update	Total number of FDB update requests sent.
failed	Total number of FDB update requests that failed.

/stats/l2/lldp <*port alias or number*>|clear

LLDP Port Statistics

```
LLDP Port INTA1 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 100. LLDP Port Statistics (/stats/l2/lldp)

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.

/stats/l2/oam

OAM Statistics

```
[OAM statistics Menu]
     port     - Show OAM port statistics
     dump     - Show all OAM statistics
```

The following table describes the OAM statistics commands:

Table 101. OAM Statistics Menu Options (/stats/l2/oam)

Command Syntax and Usage
port <*port alias or number*> Displays OAM statistics for the selected port. See page 138 for sample output.
dump Displays all OAM statistics.

/stats/l2/oam/port <*port alias or number*>
OAM Statistics

```
OAM statistics on port INTA1
----------------------------------------
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

/stats/l2/vlag
vLAG Statistics

```
[vLAG statistics Menu]
     isl      - Show vLAG ISL statistics
     clear    - Show health statistics
     dump     - Show all vLAG statistics
```

The following table describes the vLAG statistics commands:

Table 102. vLAG Statistics Menu Options (/stats/l2/vlag)

Command Syntax and Usage
`isl` Displays vLAG ISL statistics for the selected port. See page 139 for sample output.
`clear` Clears vLAG statistics.
`dump` Displays all vLAG statistics. See page 139 for sample output.

/stats/l2/vlag/isl

vLAG ISL Statistics

```
                                In Counter        Out Counter
Octets:                          2755820              2288
Packets:                           21044                26
```

ISL statistics include the total number of octets received/transmitted, and the total number of packets received/transmitted over the Inter-Switch Link (ISL).

/stats/l2/vlag/isl/dump

vLAG Statistics

```
vLAG PDU sent:
Role Election:        0         System Info:           0
Peer Instance Enable: 0         Peer Instance Disable: 0
FDB Dynamic Add:      0         FDB Dynamic Del:       0
FDB Inactive Add:     0         FDB Inactive Del:      0
Health Check:         0         ISL Hello:             0
Other:                0         Unknown:               0

vLAG PDU received:
Role Election:        0         System Info:           0
Peer Instance Enable: 0         Peer Instance Disable: 0
FDB Dynamic Add:      0         FDB Dynamic Del:       0
FDB Inactive Add:     0         FDB Inactive Del:      0
Health Check:         0         ISL Hello:             0
Other:                0         Unknown:               0

vLAG IGMP packets forwarded:
IGMP Reports:         0
IGMP Leaves:          0
```

The following table describes the vLAG statistics:

Table 103. vLAG Statistics

Statistic	Description
Role Election	Total number of vLAG PDUs sent for role elections.
System Info	Total number of vLAG PDUs sent for getting system information.
Peer Instance Enable	Total number of vLAG PDUs sent for enabling peer instance.
Peer Instance Disable	Total number of vLAG PDUs sent for disabling peer instance.
FDB Dynamic Add	Total number of vLAG PDUs sent for addition of FDB dynamic entry.
FDB Dynamic Del	Total number of vLAG PDUs sent for deletion of FDB dynamic entry.
FDB Inactive Add	Total number of vLAG PDUs sent for addition of FDB inactive entry.

Table 103. vLAG Statistics (continued)

Statistic	Description
FDB Inactive Del	Total number of vLAG PDUs sent for deletion of FDB inactive entry.
Health Check	Total number of vLAG PDUs sent for health checks.
ISL Hello	Total number of vLAG PDUs sent for ISL hello.
Other	Total number of vLAG PDUs sent for other reasons.
Unknown	Total number of vLAG PDUs sent for unknown operations.
	vLAG IGMP packets forwarded
IGMP Reports	Total number of IGMP Reports forwarded over vLAG.
IGMP Leaves	Total number of IGMP Leave messages forwarded over vLAG.

/stats/l3

Layer 3 Statistics Menu

```
[Layer 3 Statistics Menu]
     geal3    - GEA Layer 3 Stats Menu
     ip       - Show IP stats
     ip6      - Show IP6 stats
     route    - Show route stats
     route6   - Show route6 stats
     pmtu6    - Show ipv6 path mtu stats
     arp      - Show ARP stats
     dns      - Show DNS stats
     icmp     - Show ICMP stats
     tcp      - Show TCP stats
     udp      - Show UDP stats
     igmp     - Show IGMP stats
     mld      - Show MLD stats
     ospf     - OSPF stats
     ospf3    - OSPFv3 stats
     vrrp     - Show VRRP stats
     rip      - Show RIP stats
     igmpgrps - Total number of IGMP groups
     ipmcgrps - Total number of IPMC groups
     clrigmp  - Clear IGMP stats
     ipclear  - Clear IP stats
     ip6clear - Clear IP6 stats
     clrvrrp  - Clear VRRP stats
     ripclear - Clear RIP stats
     ospfclr  - Clear all OSPF stats
     ospf3clr - Clear all OSPFv3 stats
     dump     - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in Table 104, with pointers to detailed information.

Table 104. Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
`geal3` Displays the Gigabit Ethernet Aggregators (GEA) statistics menu. GEA statistics are used by service and support personnel.
`ip` Displays IP statistics. See page 144 for sample output.
`ip6` Displays IPv6 statistics. See page 146 for sample output.
`route [clear]` Displays IPv4 route statistics. See page 150 for sample output. Use the `clear` option to delete all route statistics.
`route6 [clear]` Displays IPv6 route statistics. See page 151 for sample output. Use the `clear` option to delete all route statistics.

Table 104. Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
`pmtu6` Displays IPv6 Path MTU statistics. See page 151 for sample output.
`arp` Displays Address Resolution Protocol (ARP) statistics. See page 152 for sample output.
`dns [clear]` Displays Domain Name System (DNS) statistics. See page 152 for sample output. Use the `clear` option to delete all DNS statistics.
`icmp [clear]` Displays ICMP statistics. See page 153 for sample output. Use the `clear` option to delete all ICMP statistics.
`tcp [clear]` Displays TCP statistics. See page 155 for sample output. Use the `clear` option to delete all TCP statistics.
`udp [clear]` Displays UDP statistics. See page 156 for sample output. Use the `clear` option to delete all UDP statistics.
`igmp` Displays IGMP statistics. See page 157 for sample output.
`mld` Displays the MLD statistics menu. See page 158 for menu options.
`ospf` Displays OSPF statistics. See page 161 for sample output.
`ospf3` Displays OSPFv3 statistics. See page 166 for sample output.
`vrrp` When virtual routers are configured, you can display the protocol statistics for VRRP. See page 171 for sample output.
`rip` Displays Routing Information Protocol (RIP) statistics. See page 172 for sample output.
`igmpgrps` Displays the total number of IGMP groups that are registered on the switch.

Table 104. Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
`ipmcgrps` Displays the total number of current IP multicast groups that are registered on the switch.
`clrigmp` Clears IGMP statistics.
`ipclear` Clears IPv4 statistics. Use this command with caution as it will delete all the IPv4 statistics.
`ip6clear` Clears IPv6 statistics. Use this command with caution as it will delete all the IPv6 statistics.
`clrvrrp` Clears VRRP statistics.
`ripclear` Clears Routing Information Protocol (RIP) statistics.
`ospfclr` Clears Open Shortest Path First (OSPF) statistics.
`ospf3clr` Clears OSPFv3 statistics.
`dump` 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.

/stats/l3/ip

IPv4 Statistics

```
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 105. IPv4 Statistics (stats/l3/ip)

Statistics	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
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).

Table 105. IPv4 Statistics (stats/l3/ip)

Statistics	Description
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in `ipForwDatagrams`, which meet this *no-route* criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their `Don't Fragment` flag was set.
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.

Table 105. IPv4 Statistics (stats/l3/ip)

Statistics	Description
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).

/stats/l3/ip6
IPv6 Statistics

```
    IPv6 Statistics
    ***************
144  Rcvd          0    HdrErrors     0    TooBigErrors
0    AddrErrors    0    FwdDgrams     0    UnknownProtos
0    Discards      144  Delivers      130  OutRequests
0    OutDiscards   0    OutNoRoutes   0    ReasmReqds
0    ReasmOKs      0    ReasmFails
0    FragOKs       0    FragFails     0    FragCreates
7    RcvdMCastPkt  2    SentMcastPkts 0    TruncatedPkts
0    RcvdRedirects 0    SentRedirects
    ICMP Statistics
    ***************
    Received :
33  ICMPPkts     0 ICMPErrPkt      0 DestUnreach  0 TimeExcds
0   ParmProbs    0 PktTooBigMsg    9 ICMPEchoReq  10 ICMPEchoReps
0   RouterSols   0 RouterAdv       5 NeighSols    9 NeighAdv
0   Redirects    0 AdminProhib     0 ICMPBadCode
    Sent
19  ICMPMsgs     0 ICMPErrMsgs     0 DstUnReach   0 TimeExcds
0   ParmProbs    0 PktTooBigs      10 EchoReq     9 EchoReply
0   RouterSols   0 RouterAdv       11 NeighSols   5 NeighborAdv
0   RedirectMsgs 0 AdminProhibMsgs
    UDP statistics
    **************
    Received :
0 UDPDgrams    0 UDPNoPorts       0 UDPErrPkts
    Sent :
0 UDPDgrams
```

The following table describes the IPv6 statistics.

Table 106. IPv6 Statistics (stats/l3/ip6)

Statistics	Description
`Rcvd`	Number of datagrams received from interfaces, including those received in error.
`HdrErrors`	Number of datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.

Table 106. IPv6 Statistics (stats/l3/ip6)

Statistics	Description
TooBigErrors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
AddrErrors	Number of datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses. For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
FwdDgrams	Number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
UnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	Number of IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	Number of datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).
OutNoRoutes	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ReasmReqds	Number of IP fragments received which needed to be reassembled at this entity (the switch).
ReasmOKs	Number of IP datagrams successfully re- assembled.

Table 106. IPv6 Statistics (stats/l3/ip6)

Statistics	Description
ReasmFails	Number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set.
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
RcvdMCastPkt	The number of multicast packets received by the interface.
SentMcastPkts	The number of multicast packets transmitted by the interface.
TruncatedPkts	The number of input datagrams discarded because datagram frame didn't carry enough data.
RcvdRedirects	The number of Redirect messages received by the interface.
SentRedirects	The number of Redirect messages sent.

The following table describes the IPv6 ICMP statistics.

Table 107. ICMP Statistics (stats/l3/ip6)

Statistics	Description
Received	
ICMPPkts	Number of ICMP messages which the entity (the switch) received.
ICMPErrPkt	Number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so forth).
DestUnreach	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
PktTooBigMsg	The number of ICMP Packet Too Big messages received by the interface.
ICMPEchoReq	Number of ICMP Echo (request) messages received.

Table 107. ICMP Statistics (stats/l3/ip6)

Statistics	Description
ICMPEchoReps	Number of ICMP Echo Reply messages received.
RouterSols	Number of Router Solicitation messages received by the switch.
RouterAdv	Number of Router Advertisements received by the switch.
NeighSols	Number of Neighbor Solicitations received by the switch.
NeighAdv	Number of Neighbor Advertisements received by the switch.
Redirects	Number of ICMP Redirect messages received.
AdminProhib	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPBadCode	The number of ICMP Parameter Problem messages received by the interface.
Sent	
ICMPMsgs	Number of ICMP messages which this entity (the switch) attempted to send.
ICMPErrMsgs	Number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
DstUnReach	Number of ICMP Destination Unreachable messages sent.
TimeExcds	Number of ICMP Time Exceeded messages sent.
ParmProbs	Number of ICMP Parameter Problem messages sent.
PktTooBigs	The number of ICMP Packet Too Big messages sent by the interface.
EchoReq	Number of ICMP Echo (request) messages sent.
EchoReply	Number of ICMP Echo Reply messages sent.
RouterSols	Number of Router Solicitation messages sent by the switch.
RouterAdv	Number of Router Advertisements sent by the switch.
NeighSols	Number of Neighbor Solicitations sent by the switch.
NeighAdv	Number of Neighbor Advertisements sent by the switch.
RedirectMsgs	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

Table 107. ICMP Statistics (stats/l3/ip6)

Statistics	Description
AdminProhibMsgs	Number of ICMP destination unreachable/communication administratively prohibited messages sent.

The following table describes the UDP statistics.

Table 108. UDP Statistics (stats/l3/ip6)

Statistics	Description
Received	
UDPDgrams	Number of UDP datagrams received by the switch.
UDPNoPorts	Number of received UDP datagrams for which there was no application at the destination port.
UDPErrPkts	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Sent	
UDPDgrams	Number of UDP datagrams sent from this entity (the switch).

/stats/l3/route [clear]

IPv4 Route Statistics

```
Route statistics:
----------------
Current total outstanding routes     :            1
Highest number ever recorded         :            1
Current static routes                :            0
Current RIP routes                   :            0
Current OSPF routes                  :            0
Current BGP routes                   :            0
Maximum supported routes             :         2048

ECMP statistics (active in ASIC):
--------------------------------
Maximum number of ECMP routes        :         2048
Maximum number of static ECMP routes :          128
Number of routes with ECMP paths     :            0
```

Use the `clear` option to delete all IPv4 route statistics.

/stats/l3/route6 [clear]

IPv6 Route Statistics

```
IPV6 Route statistics:
ipv6RoutesCur:               1  ipv6RoutesHighWater:         1
ipv6RoutesMax:            1880

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

Table 109. IPv6 Route Statistics (/stats/l3/route)

Statistics	Description
ipv6RoutesCur	Total number of outstanding routes in the route table.
ipv6RoutesHighWater	Highest number of routes ever recorded in the route table.
ipv6RoutesMax	Maximum number of routes that are supported.
Maximum number of ECMP routes	Maximum number of ECMP routes that are supported.
Max ECMP paths allowed for one route	Maximum number of ECMP paths supported for each route.

Use the `clear` option to delete all IPv6 route statistics.

/stats/l3/pmtu6

IPv6 Path MTU Statistics

```
Max Cache Entry Number : 10
Current Cache Entry Number: 0
```

Table 110. Path MTU Statistics (/stats/l3/pmtu6)

Statistics	Description
Max Cache Entry Number	Maximum number of Path MTU entries that are supported.
Current Cache Entry Number	Total number of Path MTU entries in the Path MTU table.

/stats/l3/arp
ARP Statistics

This menu option enables you to display Address Resolution Protocol statistics.

```
ARP statistics:
arpEntriesCur:             3  arpEntriesHighWater:          4
arpEntriesMax:          4095
```

Table 111. ARP Statistics (/stats/l3/arp)

Statistics	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.
arpEntriesMax	The maximum number of ARP entries that are supported.

/stats/l3/dns [clear]
DNS Statistics

This menu option enables you to display Domain Name System statistics.

```
DNS statistics:
dnsInRequests:             0
dnsOutRequests:            0
dnsBadRequests:            0
```

Table 112. DNS Statistics (/stats/dns)

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.

Use the `clear` option to delete all DNS statistics.

/stats/l3/icmp [clear]

ICMP Statistics

```
ICMP statistics:
icmpInMsgs:             245802   icmpInErrors:              1393
icmpInDestUnreachs:         41   icmpInTimeExcds:              0
icmpInParmProbs:             0   icmpInSrcQuenchs:             0
icmpInRedirects:             0   icmpInEchos:                 18
icmpInEchoReps:         244350   icmpInTimestamps:             0
icmpInTimestampReps:         0   icmpInAddrMasks:              0
icmpInAddrMaskReps:          0   icmpOutMsgs:             253810
icmpOutErrors:               0   icmpOutDestUnreachs:         15
icmpOutTimeExcds:            0   icmpOutParmProbs:             0
icmpOutSrcQuenchs:           0   icmpOutRedirects:             0
icmpOutEchos:           253777   icmpOutEchoReps:             18
icmpOutTimestamps:           0   icmpOutTimestampReps:         0
icmpOutAddrMasks:            0   icmpOutAddrMaskReps:          0
```

Table 113. ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by `icmpInErrors`.
icmpInErrors	The number of ICMP messages which the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	The number of ICMP Timestamp `Reply` messages received.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.

Table 113. ICMP Statistics (/stats/l3/icmp)

Statistics	Description
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by `icmpOutErrors`.
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	The number of ICMP Timestamp `Reply` messages sent.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

Use the `clear` option to delete all ICMP statistics.

/stats/l3/tcp [clear]

TCP Statistics

```
TCP statistics:
tcpRtoAlgorithm:         4   tcpRtoMin:               0
tcpRtoMax:          240000   tcpMaxConn:            512
tcpActiveOpens:     252214   tcpPassiveOpens:         7
tcpAttemptFails:       528   tcpEstabResets:          4
tcpInSegs:          756401   tcpOutSegs:         756655
tcpRetransSegs:          0   tcpInErrs:               0
tcpCurBuff:              0   tcpCurConn:              3
tcpOutRsts:            417
```

Table 114. TCP Statistics (/stats/l3/tcp)

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the `timeout` value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission `timeout`, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission `timeout`. In particular, when the `timeout` algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
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.

Table 114. TCP Statistics (/stats/l3/tcp)

Statistics	Description
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`).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.

Use the `clear` option to delete all TCP statistics.

/stats/l3/udp [clear]

UDP Statistics

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

Table 115. UDP Statistics (/stats/l3/udp)

Statistics	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.

Use the `clear` option to delete all UDP statistics.

/stats/l3/igmp <*VLAN number*>

IGMP Statistics

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

This menu option displays statistics about the use of the IGMP Multicast Groups. IGMP statistics are described in the following table:

Table 116. IGMP Statistics (/stats/l3/igmp)

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
rxIgmpGrpSpecific Queries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecific Queries	Total number of Group Source-Specific Queries (GSSQ) received
rxIgmpDiscardPkts	Total number of IGMP packets discarded
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecific Queries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave messages transmitted
rxIgmpV3CurrentState Records	Total number of Current State records received
rxIgmpV3SourceList ChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChange Records	Total number of Filter Change records received.
txIgmpGenQueries	Total number of General Membership Query packets transmitted.

/stats/l3/mld

MLD Statistics Menu

```
[MLD stats Menu]
     global   - Show global stats
     mldgrps  - Show total number of MLD entries
     if       - Show interface(s) mld stats
     clear    - Show interface(s) mld stats
```

Table 117 describes the MLD statistics menu options.

Table 117. MLD Statistics Menu (/stats/l3/mld)

Command Syntax and Usage
`global` Displays MLD global statistics. See page 159 for sample output.
`mldgrps` Displays total number of MLD entries.
`if` Displays MLD interface statistics.
`clear` Clears all MLD statistics.

/stats/l3/mld/global

MLD Global Statistics

The MLD global statistics displays information for all MLD packets received on all interfaces.

```
MLD global statistics:
----------------------
Total L3 IPv6 (S, G, V) entries:  2
Total MLD groups:                 2
Bad Length:                       0
Bad Checksum:                     0
Bad Receive If:                   0
Receive non-local:                0
Invalid Packets:                  4

MLD packet statistics for interfaces:

MLD interface packet statistics for interface 1:
MLD msg type           Received               Sent               RxErrors
------------     -------------------- -------------------- --------------------
General Query                       0                 1067                    0
MAS Query                           0                    0                    0
MASSQ Query                         0                    0                    0
MLDv1 Report                        0                    0                    0
MLDv1 Done                          0                    0                    0
MLDv2 Report                     1069                 1084                    0
INC CSRs(v2)                        1                    0                    0
EXC CSRs(v2)                     2134                 1093                    0
TO_INC FMCRs(v2)                    1                    0                    0
TO_EXC FMCRs(v2)                    0                   15                    0
ALLOW SLCRs(v2)                     0                    0                    0
BLOCK SLCRs(v2)                     0                    0                    0

MLD interface packet statistics for interface 2:
MLD msg type           Received               Sent               RxErrors
------------     -------------------- -------------------- --------------------

MLD interface packet statistics for interface 3:
MLD msg type           Received               Sent               RxErrors
------------     -------------------- -------------------- --------------------
General Query                       0                 2467                    0
MAS Query                           0                    0                    0
MASSQ Query                         0                    0                    0
MLDv1 Report                        0                    0                    0
MLDv1 Done                          0                    0                    0
MLDv2 Report                        2                 2472                    0
INC CSRs(v2)                        1                    0                    0
EXC CSRs(v2)                        0                 2476                    0
TO_INC FMCRs(v2)                    0                    0                    0
TO_EXC FMCRs(v2)                    0                    8                    0
ALLOW SLCRs(v2)                     0                    0                    0
BLOCK SLCRs(v2)                     1                    0                    0
```

The following table describes the fields in the MLD global statistics output.

Table 118. MLD Global Statistics (/stats/l3/mld/global)

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

/stats/l3/ospf

OSPF Statistics Menu

```
[OSPF stats Menu]
      general - Show global stats
      aindex  - Show area(s) stats
      if      - Show interface(s) stats
```

Table 119. OSPF Statistics Menu (/stats/l3/ospf)

Command Syntax and Usage
`general` Displays global statistics. See page 162 for sample output.
`aindex` Displays area statistics.
`if` Displays interface statistics.

/stats/l3/ospf/general

OSPF Global Statistics

The OSPF General Statistics contain the sum total of all OSPF packets received on all OSPF areas and interfaces.

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

Nbr change stats:                Intf change Stats:
  hello                  2           up                4
  start                  0           down              2
  n2way                  2           loop              0
  adjoint ok             2           unloop            0
  negotiation done       2           wait timer        2
  exchange done          2           backup            0
  bad requests           0           nbr change        5
  bad sequence           0
  loading done           2
  n1way                  0
  rst_ad                 0
  down                   1

Timers kickoff
  hello                514
  retransmit          1028
  lsa lock               0
  lsa ack                0
  dbage                  0
  summary                0
  ase export             0
```

Table 120. OSPF General Statistics (stats/l3/ospf/general)

Statistics		Description
Rx/Tx Stats:		
	Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
	Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
	Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
	Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
	Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.

Table 120. OSPF General Statistics (stats/l3/ospf/general) (continued)

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

Table 120. OSPF General Statistics (stats/l3/ospf/general) (continued)

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

Table 120. OSPF General Statistics (stats/l3/ospf/general) (continued)

Statistics		Description
Intf Change Stats:		
	up	The sum total number of interfaces up in all OSPF areas.
	down	The sum total number of interfaces down in all OSPF areas.
	loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
	unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
	wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
	backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
	nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.
Timers Kickoff:		
	hello	The sum total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OPSF areas and interfaces.
	retransmit	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
	lsa lock	The sum total number of times the Link State Advertisement (LSA) lock timer has been fired across all OSPF areas and interfaces.
	lsa ack	The sum total number of times the LSA `Ack` timer has been fired across all OSPF areas and interfaces.
	dbage	The total number of times the data base age (`Dbage`) has been fired.
	summary	The total number of times the Summary timer has been fired.
	ase export	The total number of times the Autonomous System Export (ASE) timer has been fired.

/stats/l3/ospf3

OSPFv3 Statistics Menu

```
[OSPFV3 stats Menu]
      general - Show global stats
      aindex  - Show area(s) stats
      if      - Show interface(s) stats
```

Table 121. OSPFv3 Statistics Menu (/stats/l3/ospf3)

Command Syntax and Usage
`general` Displays global statistics. See page 167 for sample output.
`aindex` Displays area statistics.
`if` Displays interface statistics.

/stats/l3/ospf3/general

OSPFv3 Global Statistics

```
OSPFv3 stats
----------
Rx/Tx/Disd Stats:          Rx            Tx         Discarded
                        --------      --------      ---------
       Pkts               9695          95933             0
       hello              9097           8994             0
       database             39             51             6
       ls requests          16              8             0
       ls acks             172            360             0
       ls updates          371            180             0

Nbr change stats:                Intf change Stats:
  down                    0            down               5
  attempt                 0            loop               0
  init                    1            waiting            6
  n2way                   1            ptop               0
  exstart                 1            dr                 4
  exchange done           1            backup             6
  loading done            1            dr other           0
  full                    1            all events        33
  all events              6

Timers kickoff
  hello                8988
  wait                 6
  poll                 0
  nbr probe            0

Number of LSAs
  originated                      180
  rcvd newer originations         355
```

The OSPFv3 General Statistics contain the sum total of all OSPF packets received on all OSPFv3 areas and interfaces.

Table 122. OSPFv3 General Statistics (stats/l3/ospf3/general)

Statistics		Description
Rx/Tx Stats:		
	Rx Pkts	The sum total of all OSPFv3 packets received on all OSPFv3 interfaces.
	Tx Pkts	The sum total of all OSPFv3 packets transmitted on all OSPFv3 interfaces.
	Discarded Pkts	The sum total of all OSPFv3 packets discarded.
	Rx hello	The sum total of all Hello packets received on all OSPFv3 interfaces.
	Tx hello	The sum total of all Hello packets transmitted on all OSPFv3 interfaces.
	Discarded hello	The sum total of all Hello packets discarded, including packets for which no associated interface has been found.

Table 122. OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics		Description
	Rx database	The sum total of all Database Description packets received on all OSPFv3 interfaces.
	Tx database	The sum total of all Database Description packets transmitted on all OSPFv3 interfaces.
	Discarded database	The sum total of all Database Description packets discarded.
	Rx ls requests	The sum total of all Link State Request packets received on all OSPFv3 interfaces.
	Tx ls requests	The sum total of all Link State Request packets transmitted on all OSPFv3 interfaces.
	Discarded ls requests	The sum total of all Link State Request packets discarded.
	Rx ls acks	The sum total of all Link State Acknowledgement packets received on all OSPFv3 interfaces.
	Tx ls acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPFv3 interfaces.
	Discarded ls acks	The sum total of all Link State Acknowledgement packets discarded.
	Rx ls updates	The sum total of all Link State Update packets received on all OSPFv3 interfaces.
	Tx ls updates	The sum total of all Link State Update packets transmitted on all OSPFv3 interfaces.
	Discarded ls updates	The sum total of all Link State Update packets discarded.
Nbr Change Stats:		
	down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPFv3 interfaces.
	attempt	The total number of transitions into attempt state of neighboring routers across all OSPFv3 interfaces.
	init	The total number of transitions into init state of neighboring routers across all OSPFv3 interfaces.
	n2way	The total number of bidirectional communication establishment between this router and other neighboring routers.
	exstart	The total number of transitions into exstart state of neighboring routers across all OSPFv3 interfaces

Table 122. OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics		Description
	exchange done	The total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPFv3 interfaces.
	loading done	The total number of link state updates received for all out-of-date portions of the database across all OSPFv3 interfaces.
	full	The total number of transitions into full state of neighboring routers across all OSPFv3 interfaces.
	all events	The total number of state transitions of neighboring routers across all OSPFv3 interfaces.

Table 122. OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics		Description
Intf Change Stats:		
	down	The total number of transitions into down state of all OSPFv3 interfaces.
	loop	The total number of transitions into loopback state of all OSPFv3 interfaces.
	waiting	The total number of transitions into waiting state of all OSPFv3 interfaces.
	ptop	The total number of transitions into point-to-point state of all OSPFv3 interfaces.
	dr	The total number of transitions into Designated Router other state of all OSPFv3 interfaces.
	backup	The total number of transitions into backup state of all OSPFv3 interfaces.
	all events	The total number of changes associated with any OSPFv3 interface, including changes into internal states.
Timers Kickoff:		
	hello	The total number of times the Hello timer has been fired (which triggers the `send` of a Hello packet) across all OSPFv3 interfaces.
	wait	The total number of times the wait timer has been fired (which causes an interface to exit waiting state), across all OPSFv3 interfaces.
	poll	The total number of times the timer whose firing causes hellos to be sent to inactive NBMA and Demand Circuit neighbors has been fired, across all OPSFv3 interfaces.
	nbr probe	The total number of times the neighbor probe timer has been fired, across all OPSFv3 interfaces.
Number of LSAs:		
	originated	The number of LSAs originated by this router.
	rcvd newer originations	The number of LSAs received that have been determined to be newer originations.

/stats/l3/vrrp

VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the CN4093 10Gb Converged Scalable Switch (CN4093) provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

When virtual routers are configured, you can display the protocol statistics for VRRP:

```
VRRP statistics:
vrrpInAdvers:             0   vrrpBadAdvers:                0
vrrpOutAdvers:            0   vrrpOutGratuitousARPs:        0
vrrpBadVersion:           0   vrrpBadVrid:                  0
vrrpBadAddress:           0   vrrpBadData:                  0
vrrpBadPassword:          0   vrrpBadInterval:              0
```

Table 123. VRRP Statistics (/stats/l3/vrrp)

Statistics	Description
vrrpInAdvers	The total number of valid VRRP advertisements that have been received.
vrrpBadAdvers	The total number of VRRP advertisements received that were dropped.
vrrpOutAdvers	The total number of VRRP advertisements that have been sent.
vrrpOut GratuitousARPs	The total number of VRRP gratuitous ARPs that have been sent.
vrrpBadVersion	The total number of VRRP advertisements received that had a bad version number.
vrrpBadVrid	The total number of VRRP advertisements received that had a bad virtual router ID.
vrrpBadAddress	The total number of VRRP advertisements received that had a bad address.
vrrpBadData	The total number of VRRP advertisements received that had bad data.
vrrpBadPassword	The total number of VRRP advertisements received that had a bad password.
vrrpBadInterval	The total number of VRRP advertisements received that had a bad interval.

/stats/l3/rip

Routing Information Protocol Statistics

```
RIP ALL STATS INFORMATION:
        RIP packets received  = 12
        RIP packets sent      = 75
        RIP request received  = 0
        RIP response recevied = 12
        RIP request sent      = 3
        RIP reponse sent      = 72
        RIP route timeout     = 0
        RIP bad size packet received = 0
        RIP bad version received       = 0
        RIP bad zeros received         = 0
        RIP bad src port received      = 0
        RIP bad src IP received        = 0
        RIP packets from self received = 0
```

/stats/mp

Management Processor Statistics Menu

```
[MP-specific Statistics Menu]
     thr      - Show STEM thread stats
     nthr     - Show new STEM thread stats
     i2c      - Show I2C stats
     pkt      - Show Packet stats
     tcb      - Show All TCP control blocks in use
     ucb      - Show All UDP control blocks in use
     cpu      - Show CPU utilization
     ncpu     - Show new CPU utilization
     hcpu     - Show history of CPU utilization
     mem      - Show Memory utilization stats
```

Table 124. Management Processor Statistics Menu Options (/stats/mp)

Command Syntax and Usage
`thr` Displays STEM thread statistics. This command is used by Technical Support personnel.
`nthr` Displays new STEM thread statistics. This command is used by Technical Support personnel.
`i2c` Displays I2C statistics. This command is used by Technical Support personnel.
`pkt` Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 173.
`tcb` Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 183.
`ucb` Displays all UDP control blocks that are in use. To view a sample output, see page 184.
`cpu` Displays CPU use for all threads for periods of 1 second, 5 second, 1 minute, and 5 minutes. To view a sample output and a description of the stats, see page 184.
`hcpu` Displays history of CPU utilization. To view a sample output, see page 185.
`mem` Displays system memory statistics.

/stats/mp/pkt

Packet Statistics Menu

```
[MP Packet Statistics Menu]
     counters - Show packet counters
     clear    - Clear all CPU packet statistics and logs
     logs     - Display log of all packets received by CPU
     last     - Display log of last the N packets received by CPU
     dump     - Dump all packet statistics and logs
     parse    - MP Packet Parse Menu
```

The following table describes the packet statistics menu options.

Table 125. Packet Statistics Menu Options (/stats/mp/pkt)

Command Syntax and Usage
`counters` Displays packet statistics, to check for leads and load. To view a sample output and a description of the statistics, see page 175.
`clear` Clears all CPU packet statistics and logs.
`logs` Displays the CPU packet statistics Logs menu. See page 179 to view menu options.
`last` Displays the packet statistics Last Packets menu. See page 180 to view menu options.
`dump` Displays the packet statistics Dump menu. See page 181 to view menu options.
`parse` Displays the packet statistics Parse menu. See page 181 to view menu options.

/stats/mp/pkt/counters

MP Packet Statistics

```
CPU packet statistics at  0:13:36 Thu Mar 15, 2012

Packet rate:         Incoming            Outgoing
------------         --------            --------
1-second:                   5                   2
4-seconds:                  5                   1
64-seconds:                 5                   1

Packet counters:     Received                Sent
-----------------    --------                ----
Total packets:         359841              103895
Since bootup:          359841              103895

BPDUs:                  32240               32498
Cisco packets:              0                   0
ARP packets:           217226                   0
LACP packets:               0                   0
IPv4 packets:           88129               71397
 IGMP packets:              0                   0
 PIM packets:               0                   0
 ICMP Requests:             0               63586
 ICMP Replies:          63186                   0
 TCP  packets:              0                   0
  FTP                       0                   0
  HTTP                      0                   0
  SSH                       0                   0
  TACACS                    0                   0
  TELNET                    0                   0
  TCP other                 0                   0

 UDP packets:           28758                7811
  DHCP                  24872                7800
  NTP                      63                   0
  RADIUS                    0                   0
  SNMP                   3823                  11
  TFTP                      0                   0
  UDP other                63                   0
 RIP packets:               0                   0
 OSPF packets:              0                   0
 BGP packets:               0                   0
IPv6 packets:           22246                   0
LLDP PDUs:                  0                   0
ECP PDUs:                   0                   0
MgmtSock Packets:       63197               71397
Other:                      0                   0
...
```

```
 CPU packet statistics at  0:13:36 Thu Mar 15, 2012

Packet Buffer Statistics:
-------------------------
 allocs:        483682
 frees:         483681
 failures:           0
 dropped:            0

 small packet buffers:
 ----------------------
   current:                  0
   max:                   2048
   threshold:              512
   hi-watermark:             4
   hi-water time:    6:15:29 Wed Mar 14, 2012

 medium packet buffers:
 ----------------------
   current:                  1
   max:                   2048
   threshold:              512
   hi-watermark:             3
   hi-water time:    6:15:18 Wed Mar 14, 2012

 jumbo packet buffers:
 ----------------------
   current:                  0
   max:                      4
   hi-watermark:             0

 pkt_hdr statistics:
 ----------------------
 current          :           0
 max              :        3072
 hi-watermark     :           4
```

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 and sent.
Since bootup	Total number of packets received and sent since the last switch reboot.

Statistics	Description
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received and sent.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received and sent.
ARP packets	Total number of Address Resolution Protocol packets received and sent.
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.
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 and sent.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received and sent.
ECP PDUs	Total number of Edge Control Protocol data units received and sent.

Statistics	Description
MgmtSock Packets	Total number of packets received and transmitted through the management port.
Other	Total number of other packets received and transmitted.
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.
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.

Statistics	Description
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 allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack that are 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.

/stats/mp/pkt/logs
Packet Statistics Log Menu

```
[MP Packet Logs Menu]
     all      - Display logs of all packets received/sent by CPU
     rx       - Display logs of packets received by CPU
     tx       - Display logs of packets sent by CPU
```

This menu allows you to display a log of all packets received by CPU. The following table describes the Packet Statistics Log menu options.

Table 126. Packet Statistics Log Menu Options (/stats/mp/pkt/log)

Command Syntax and Usage
`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 page 180.
`rx` Displays all packets logs received by the CPU.
`tx` Displays all packet logs sent from the CPU.

/stats/mp/pkt/logs/all
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

/stats/mp/pkt/last
Packet Statistics Last Packet Menu

```
[MP Packet Last Packet Menu]
     both     - Display logs of the last N packets received/sent by CPU
     rx       - Display logs of the last N packets received by CPU
     tx       - Display logs of the last N packets sent by CPU
```

This menu allows 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 menu options.

Table 127. Last Packet Menu Options (/stats/mp/pkt/last)

Command Syntax and Usage
`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 page 180.
`rx` *<1-1000>* Displays a specified number of recent packet logs received by the CPU.
`tx` *<1-1000>* Displays a specified number of recent packet logs sent from the CPU.

/stats/mp/pkt/dump

Packet Statistics Dump Menu

```
[MP Packet Dump Menu]
     all      - Display packet statistics and all logs
     rx       - Display packet statistics and received logs
     tx       - Display packet statistics and sent logs
```

The following table describes the Packet Statistics Dump menu options.

Table 128. Packet Dump Menu Options (/stats/mp/pkt/dump)

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

/stats/mp/pkt/parse

Packet Statistics Parse Menu

```
[MP Packet Parse Menu]
     rx       - Display Receive packets parsed
     tx       - Display Sent packets parsed
```

The following table describes the Packet Statistics Parse menu options.

Table 129. Packet Parse Menu Options (/stats/mp/pkt/parse)

Command Syntax and Usage
`rx` *<packet type>* Displays specified packet types received by the CPU. Table 130 lists the packet types accepted by this command.
`tx` *<packet type* Displays specified packet types sent from the CPU. Table 130 lists the packet types accepted by this command.

Table 130. Packet types accepted by the packet parse command

Packet Type	Description
arp	Display only ARP packets logged.
bgp	Display only BGP packets logged.
bpdu	Display only BPDUs logged.
cisco	Display only Cisco packets (BPDU/CDP/UDLD) logged.

Packet Type	Description
dhcp	Display only DHCP packets logged.
ecp	Display only ECP packets logged.
fcoe	Display only FCoE FIP PDUs logged.
ftp	Display only FTP packet logged.
http	Display only HTTP packets logged.
icmp	Display only ICMP packets logged.
igmp	Display only IGMP packet logged.
ip-addr	Display only logged packets with specified IP address.
ipv4	Display only IPv4 packets logged.
ipv6	Display only IPv6 packets logged.
lacp	Display only LACP packets logged.
lldp	Display only LLDP PDUs logged.
mac	Display only logged packets with specified MAC address.
mgmtsock	Display only packets logged from management ports.
ntp	Display only NTP packets logged.
ospf	Display only OSPF packet logged.
other	Display logs of all packets not explicitly selectable.
pim	Display only PIM packet logged.
port	Display only logged packets with specified port.
radius	Display only RADIUS packets logged.
rarp	Display only Reverse-ARP packets logged.
raw	Display raw packet buffer in addition to headers.
rip	Display only RIP packet logged.
snmp	Display only SNMP packets logged.
ssh	Display only SSH packets logged.
tacacs	Display only TACACS packets logged.
tcp	Display only TCP packets logged.
tcpother	Display only TCP other-port packets logged.
telnet	Display only TELNET packets logged.
tftp	Display only TFTP packets logged.
udp	Display only UDP packets logged.
udpother	Display only UDP other-port packets logged.
vlan	Display only logged packets with specified VLAN.

/stats/mp/tcb

TCP Statistics

```
Data Ports:
------------------------------------------------------------------
All TCP allocated control blocks:
1550c2c8:  0.0.0.0                                    0 <=>
           10.43.95.162                             443 listen MGT1 up
154c0f90:  0:0:0:0:0:0:0:0                            0 <=>
           0:0:0:0:0:0:0:0                          443  listen
154c1c98:  0.0.0.0                                    0 <=>
           0.0.0.0                                  443  listen
154c3d80:  0.0.0.0                                    0 <=>
...
Mgmt Ports:
------------------------------------------------------------------
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.43.95.162:http       *:*                     LISTEN
tcp        0      0 10.43.96.33:http        *:*                     LISTEN
tcp        0      0 10.43.95.162:ssh        *:*                     LISTEN
...
```

Table 131. MP Specified TCP Statistics

Statistics	Description
1550c2c8	Memory
0.0.0.0	Destination IP address
0	Destination port
0.0.0.0/10.43.95.162	Source IP
443	Source port
listen/MGT1 up	State

Table 132. MP Specified TCP Statistics (/stats/mp/tcb)

Statistics	Description
10ad41e8/10ad5790	Memory
0.0.0.0/47.81.27.5	Destination IP address
0/1171	Destination port
0.0.0.0/47.80.23.243	Source IP
80/23	Source port
listen/established	State

/stats/mp/ucb
UCB Statistics

```
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
```

/stats/mp/cpu
New CPU Statistics

```
Total CPU Utilization: For 1 second: 0.55%
                       For 5 second: 0.37%
                       For 1 minute: 0.40%
                       For 5 minute: 0.76%
Highest CPU Utilization: thread 110 (ETMR) at  8:02:12 Fri Oct 19, 2012
------------------------------------------------------------------------
Thread  Thread                    Utilization                  Status
  ID     Name        1sec       5sec       1Min       5Min
------------------------------------------------------------------------
  1      STEM       0.00%      0.00%      0.00%      0.00%       idle
  2      STP        0.07%      0.04%      0.04%      0.04%       idle
  3      MFDB       0.00%      0.00%      0.00%      0.00%       idle
  4      TND        0.00%      0.00%      0.00%      0.00%       idle
  5      CONS       0.00%      0.01%      0.00%      0.35%    running
...
126      NORM       0.00%      0.00%      0.00%      0.00%       idle
127      DONE       0.00%      0.00%      0.00%      0.00%       idle
```

CPU statistics provide detailed information about utilization rates over time for each CPU thread.

Table 133. CPU Statistics

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

Table 133. CPU Statistics

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

/stats/mp/hcpu

History of CPU Statistics

```
CPU Utilization History
-----------------------------------------------
  4 (TND ) 100% at  16:00:27 Wed Dec 31, 2012
127 (DONE) 100% at   1:34:43 Wed Mar  7, 2012
 20 (EPI )  55% at   1:34:53 Wed Mar  7, 2012
110 (ETMR)  56% at   1:34:54 Wed Mar  7, 2012
110 (ETMR)  64% at   1:34:56 Wed Mar  7, 2012
110 (ETMR)  68% at   1:35:01 Wed Mar  7, 2012
 94 (PROX)  75% at   2:46:54 Wed Mar  7, 2012
 94 (PROX)  84% at   2:46:55 Wed Mar  7, 2012
 94 (PROX)  84% at   2:46:57 Wed Mar  7, 2012
```

/stats/acl

ACL Statistics Menu

```
[ACL Menu]
     acl      - Display ACL stats
     acl6     - Display IPv6 ACL stats
     dump     - Display all available ACL stats
     macl     - Display MACL stats
     vmap     - Display VMAP stats
     clracl   - Clear ACL stats
     clracl6  - Clear IPv6 ACL stats
     clrmacl  - Clear MACL stats
     clrvmap  - Clear VMAP stats
```

ACL statistics are described in the following table.

Table 134. ACL Statistics Menu Options (/stats/acl)

Command Syntax and Usage
`acl` *<ACL number>* Displays the Access Control List Statistics for a specific ACL. For details, see page 187.
`acl6` *<ACL number>* Displays the IPv6 Access Control List Statistics for a specific ACL.
`macl` *<ACL number>* Displays the Management Access Control List (MACL) Statistics for a specific ACL.
`dump` Displays all ACL statistics.
`vmap` *<VMAP number>* Displays the VLAN Map statistics for a specific VMAP. For details, see page 187.
`clracl` Clears all ACL statistics.
`clracl6` Clears all IPv6 ACL statistics.
`clrmacl` Clears all Management ACL (MACL) statistics.
`clrvmap` Clears all VMAP statistics.

/stats/acl/acl [<*ACL number*>]

ACL Statistics List

This option displays statistics for the selected ACL if an ACL number is specified, or for all ACLs if the option is omitted.

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

/stats/acl/vmap [<*VMAP number*>|all]

VLAN Map Statistics

This option displays statistics for the selected VLAN Map, or for all VMAPs.

```
Hits for VMAP 1:                 57515
Hits for VMAP 2:                 74970
```

/stats/acl/meter <meter number>

ACL Meter Statistics

This option displays ACL meter statistics.

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

/stats/fcoe [clear]

Fiber Channel over Ethernet Statistics

```
FCOE statistics:
FCFAdded:                    5   FCFRemoved:                  1
FCOEAdded:                  81   FCOERemoved:                24
```

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

Table 135. FCoE Statistics (/stats/fcoe)

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

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

/stats/snmp [clear]

SNMP Statistics

Note: You can reset the SNMP counter to zero by using `clear` command, as follows:
>> Statistics# `snmp clear`

```
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 136. SNMP Statistics (/stats/snmp)

Statistics	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.
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.

Table 136. SNMP Statistics (/stats/snmp) (continued)

Statistics	Description
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`.
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.

Table 136. SNMP Statistics (/stats/snmp) (continued)

Statistics	Description
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.
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.

Table 136. SNMP Statistics (/stats/snmp) (continued)

Statistics	Description
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.

/stats/ntp
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.

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

        Last update based on response from primary/secondary server.
        Last update time: 18:04:16 Tue Jan 13, 2012
        Current system time: 18:55:49 Tue Jan 13, 2012
```

Table 137. NTP Statistics Parameters (/stats/ntp)

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.
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: `/stats/ntp`

Note: Use the following command to delete all NTP statistics: `/stats/ntp clear`

`/stats/dump`

Statistics Dump

Use the dump command to dump all switch statistics available from the Statistics Menu (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 commands.

Chapter 5. The Configuration Menu

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.

/cfg
Configuration Menu

```
[Configuration Menu]
     sys      - System-wide Parameter Menu
     port     - Port Menu
     qos      - QOS Menu
     acl      - Access Control List Menu
     pmirr    - Port Mirroring Menu
     l2       - Layer 2 Menu
     l3       - Layer 3 Menu
     cee      - CEE Configuration Menu
     fcoe     - Fiber Channel Over Ethernet Configuration Menu
     rmon     - RMON Menu
     virt     - Virtualization Menu
     setup    - Step by step configuration set up
     dump     - Dump current configuration to script file
     ptcfg    - Backup current configuration to FTP/SFTP/TFTP server
     gtcfg    - Restore current configuration from FTP/SFTP/TFTP server
     cur      - Display current configuration
```

Each configuration option is briefly described in Table 138, with pointers to detailed menu commands.

Table 138. Configuration Menu Options (/cfg)

Command Syntax and Usage
`sys` Displays the System Configuration Menu. To view menu options, see page 196.
`port` *<port alias or number>* Displays the Port Configuration Menu. To view menu options, see page 232.
`qos` Displays the Quality of Service Configuration Menu. To view menu options, see page 243.
`acl` Displays the ACL Configuration Menu. To view menu options, see page 245.
`pmirr` Displays the Mirroring Configuration Menu. To view menu options, see page 264.

Table 138. Configuration Menu Options (/cfg) (continued)

Command Syntax and Usage
`l2` Displays the Layer 2 Configuration Menu. To view menu options, see page 266.
`l3` Displays the Layer 3 Configuration Menu. To view menu options, see page 310.
`cee` Displays the Converged Ethernet Configuration menu. To view menu options, see page 404.
`fcoe` Displays the Fiber Channel over Ethernet Configuration menu. To view menu options, see page 411.
`rmon` Displays the Remote Monitoring (RMON) Configuration Menu. To view menu options, see page 413.
`virt` Displays the Virtualization Configuration Menu. To view menu options, see page 417.
`dump` Dumps current configuration to a script file. For details, see page 431.
`ptcfg` *<FTP/TFTP/SFTP server host name or IP address> <filename on host>* Backs up current configuration to FTP/TFTP/SFTP server. For details, see page 432.
`gtcfg` *<host name or IP address of FTP/TFTP/SFTP server> <filename on host>* Restores current configuration from FTP/TFTP/SFTP server. For details, see page 432.
`cur` Displays current configuration parameters.

Viewing, Applying, and Saving Changes

As you use the configuration menus to set switch parameters, the changes you make do not take effect immediately. All changes are considered “pending” until you explicitly apply them. Also, any changes are lost the next time the switch boots unless the changes are explicitly saved.

Note: Some operations can override the settings in the Configuration menu. Therefore, settings you view in the Configuration menu (for example, port status) might differ from run-time information that you view in the Information menu or on the management module. The Information menu displays current run-time information of switch parameters.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Save the changes to flash memory

Viewing Pending Changes

You can view all pending configuration changes by entering `diff` at the menu prompt.

Note: The `diff` command is a global command. Therefore, you can enter `diff` at any prompt in the CLI.

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply configuration changes, enter `apply` at any prompt in the CLI.

```
# apply
```

Note: The `apply` command is a global command. Therefore, you can enter `apply` at any prompt in the administrative interface.

Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the CN4093 10Gb Converged Scalable Switch (CN4093).

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 at any CLI prompt:

```
# save
```

When you save configuration changes, the changes are saved to the *active* configuration block. The configuration being replaced by the save is first copied to the *backup* configuration block. If you do not want the previous configuration block copied to the backup configuration block, enter the following instead:

```
# save n
```

You can decide which configuration you want to run the next time you reset the switch. Your options include:

- The active configuration block
- The backup configuration block
- Factory default configuration

You can view all pending configuration changes that have been applied but not saved to flash memory using the `diff flash` command. It is a global command that can be executed from any menu.

For instructions on selecting the configuration to run at the next system reset, see “Selecting a Configuration Block” on page 457.

/cfg/sys
System Configuration Menu

```
[System Menu]
     errdis   - ErrDisable Menu
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ldap     - LDAP Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     dst      - Custom DST Menu
     sflow    - sFlow Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone (daylight savings)
     dlight   - Set system daylight savings
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     reminder - Enable/disable Reminders
     rstctrl  - Enable/disable System reset on panic
     cur      - Display current system-wide parameters
```

This menu provides configuration of switch management parameters such as user and administrator privilege mode passwords, Web-based management settings, and management access lists.

Table 139. System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`errdis` Displays the Error Disable Recovery menu. To view menu options, see page 198.
`syslog` Displays the Syslog Menu. To view menu options, see page 200.
`sshd` Displays the SSH Server Menu. To view menu options, see page 202.
`radius` Displays the RADIUS Authentication Menu. To view menu options, see page 203.
`tacacs+` Displays the TACACS+ Authentication Menu. To view menu options, see page 204.
`ldap` Displays the LDAP Authentication Menu. To view menu options, see page 207.

Table 139. System Configuration Menu Options (/cfg/sys) (continued)

Command Syntax and Usage
`ntp` Displays the NTP Server menu, which allows you to synchronize the switch clock with a Network Time Protocol server. To view menu options, see page 209.
`ssnmp` Displays the System SNMP Menu. To view menu options, see page 211.
`access` Displays the System Access Menu. To view menu options, see page 223.
`dst` Displays the Custom Daylight Savings Time menu. To view menu options, see page 229.
`sflow` Displays the sFlow menu. To view menu options, see page 230.
`date` Prompts the user for the system date. The date retains its value when the switch is reset.
`time` Configures the system time using a 24-hour clock format. The time retains its value when the switch is reset.
`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 Savings Time, etc.
`dlight enable|disable` Disables or enables daylight savings 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. The default value is `disabled`.
`idle` *<idle timeout in minutes>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes. A value of 0 disables system idle.
`notice` *<maximum 1024 character multi-line login notice>* *<'.' to end>* Displays login notice immediately before the “Enter password:” prompt. This notice can contain up to 1024 characters and new lines.
`bannr` *<string, maximum 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 `/info/sys` command.

Table 139. System Configuration Menu Options (/cfg/sys) (continued)

Command Syntax and Usage
`hprompt disable|enable` Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).
`reminder disable|enable` Enables or disables reminder messages in the CLI. The default value is `enabled`.
`rstctrl disable|enable` 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. The default value is `enabled`.
`cur` Displays the current system parameters.

/cfg/sys/errdis
Error Disable Configuration

```
[System ErrDisable Menu]
     lfd      - Link Flap Dampening Menu
     timeout  - Set ErrDisable timeout (sec)
     ena      - Enable ErrDisable recovery
     dis      - Disable ErrDisable recovery
     cur      - Display current ErrDisable 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 140. Error Disable Configuration Options

Command Syntax and Usage
`lfd` Displays the Link Flap Dampening menu. To view menu options, see page 198.
`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.

Table 140. Error Disable Configuration Options

Command Syntax and Usage
`ena` 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 (`/cfg/port` *x*`/errdis/ena`).
`dis` Globally disables error-recovery for error-disabled ports.
`cur` Displays the current system Error Disable and Recovery configuration.

/cfg/sys/errdis/lfd
Link Flap Dampening Menu

```
[Link Flap Dampening Menu]
     flaps    - Set maximum number of flaps allowed in time period
     time     - Set time period to count flaps (sec)
     ena      - Enable Link Flap Dampening
     dis      - Disable Link Flap Dampening
     cur      - Display current Link Flap Dampening configuration
```

Table 141. Link Flap Dampening Configuration Options

Command Syntax and Usage
`flaps` *<1 - 100>* Sets the maximum number of flaps allowed in a time period.
`time` *<5 - 500>* Sets the time period, in seconds, to count flaps.
`ena` Enables Link Flap Dampening.
`dis` Disables Link Flap Dampening.
`cur` Displays the current Link Flap Dampening configuration.

/cfg/sys/syslog
System Host Log Configuration Menu

```
[Syslog Menu]
     host     - Set IP address of first syslog host
     host2    - Set IP address of second syslog host
     sever    - Set the severity of first syslog host
     sever2   - Set the severity of second syslog host
     facil    - Set facility of first syslog host
     facil2   - Set facility of second syslog host
     sloopif  - Set source loopback interface index
     console  - Enable/disable console output of syslog messages
     consev   - Severity Level of console output of syslog messages
     log      - Enable/disable sysloggging of features
     buffer   - Buffer Menu
     cur      - Display current syslog settings
```

Table 142. Host Log Menu Options (/cfg/sys/syslog)

Command Syntax and Usage
`host` *<new syslog host IP address>* Sets the IP address of the first syslog host.
`host2` *<new syslog host IP address>* Sets the IP address of the second syslog host.
`sever` ***<syslog host local severity (0–7)>*** This option sets the severity level of the first syslog host displayed. The default is 7, which means log all severity levels.
`sever2` ***<syslog host local severity (0–7)>*** This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all severity levels.
`facil` ***<syslog host local facility (0-7)>*** This option sets the facility level of the first syslog host displayed. The default value is 0.
`facil2` ***<syslog host local facility (0-7)>*** This option sets the facility level of the second syslog host displayed. The default value is 0.
`sloopif` ***<1-5>*** Sets the loopback interface number for syslogs.
`console disable|enable` Enables or 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.
`consev` ***<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.

Table 142. Host Log Menu Options (/cfg/sys/syslog) (continued)

Command Syntax and Usage
`log <`*feature*`|all> <enable|disable>` Displays a list of features for which syslog messages can be generated. You can choose to enable or disable specific features (such as `vlans`, `stg`, or `ssh`), or to enable or disable syslog on all available features.
`buffer` Displays the system log Buffer menu. To view menu options, see page 201.
`cur` Displays the current syslog settings.

/cfg/sys/syslog/buffer
Syslog Log Buffer Configuration

```
[Buffer Menu]
     severity - Severity level of syslog messages write to flash
```

The System Log Buffer menu commands allow you to configure which severity levels to write to flash memory for later retrieval.

Table 143. Syslog Log Buffer Options (/cfg/sys/syslog/buffer)

Command Syntax and Usage
`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.

/cfg/sys/sshd
SSH Server Configuration Menu

```
[SSHD Menu]
     scpadm   - Set SCP-only admin password
     hkeygen  - Generate the RSA host key
     sshport  - Set SSH server port number
     ena      - Enable the SCP apply and save
     dis      - Disable the SCP apply and save
     on       - Turn SSH server ON
     off      - Turn SSH server OFF
     cur      - Display current SSH server configuration
```

For the CN4093, this menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see page 431).

Table 144. SSH Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage
`intrval` *<0 - 24>* Set the interval, in hours, for auto-generation of the RSA server key.
`scpadm` Set the administration password for SCP access.
`hkeygen` Generate the RSA host key.
`skeygen` Generate the RSA server key.
`sshport` *<TCP port number>* Sets the SSH server port number.
`ena` Enables the SCP apply and save.
`dis` Disables the SCP apply and save.
`on` Enables the SSH server.
`off` Disables the SSH server.
`cur` Displays the current SSH server configuration.

/cfg/sys/radius

RADIUS Server Configuration Menu

```
[RADIUS Server Menu]
    prisrv  - Set primary RADIUS server address
    secsrv  - Set secondary RADIUS server address
    secret  - Set RADIUS secret
    secret2 - Set secondary RADIUS server secret
    port    - Set RADIUS port
    retries - Set RADIUS server retries
    timeout - Set RADIUS server timeout
    sloopif  - Set RADIUS source loopback interface
    bckdoor - Enable/disable RADIUS backdoor for telnet/ssh/http/https
    secbd   - Enable/disable RADIUS secure backdoor for
              telnet/ssh/http/https
    on      - Turn RADIUS authentication ON
    off     - Turn RADIUS authentication OFF
    cur     - Display current RADIUS configuration
```

Table 145. RADIUS Server Configuration Menu Options (/cfg/sys/radius)

Command Syntax and Usage
`prisrv` *<IP address>* Sets the primary RADIUS server address.
`secsrv` *<IP address>* Sets the secondary RADIUS server address.
`secret` *<1-32 character secret>* This is the shared secret between the switch and the RADIUS server(s).
`secret2` *<1-32 character secret>* This is the secondary shared secret between the switch and the RADIUS server(s).
`port` *<RADIUS port>* Enter the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.
`retries` *<RADIUS server retries (1-3)>* Sets the number of failed authentication requests before switching to a different RADIUS server. The default is 3 requests.
`timeout` *<RADIUS server timeout seconds (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.
`sloopif` *<1-5>* Sets the RADIUS source loopback interface.
`bckdoor disable|enable` 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.

Table 145. RADIUS Server Configuration Menu Options (/cfg/sys/radius) (continued)

Command Syntax and Usage
`secbd enable|disable` Enables or disables the RADIUS back door using secure password for telnet/SSH/HTTP/HTTPS. This command does not apply when backdoor (`telnet`) is enabled.
`on` Enables the RADIUS server.
`off` Disables the RADIUS server.
`cur` Displays the current RADIUS server parameters.

/cfg/sys/tacacs+
TACACS+ Server Configuration Menu

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.

```
[TACACS+ Server Menu]
    prisrv   - Set IP address of primary TACACS+ server
    secsrv   - Set IP address of secondary TACACS+ server
    chpass_p - Set new password for primary server
    chpass_s - Set new password for secondary server
    secret   - Set secret for primary TACACS+ server
    secret2  - Set secret for secondary TACACS+ server
    port     - Set TACACS+ port number
    retries  - Set number of TACACS+ server retries
    attempts - Set number of TACACS+ login attempts
    timeout  - Set timeout value of TACACS+ server retries
    sloopif  - Set TACACS+ source loopback interface
    usermap  - Set user privilege mappings
    bckdoor  - Enable/disable TACACS+ backdoor for telnet/ssh/http/hhtps
    secbd    - Enable/disable TACACS+ secure backdoor
    cmap     - Enable/disable TACACS+ new privilege level mapping
    passch   - Enable/disable TACACS+ password change
    cauth    - Enable/disable TACACS+ command authorization
    clog     - Enable/disable TACACS+ command logging
    dreq     - Enable/disable TACACS+ directed request
    acct     - Enable/disable TACACS+ accounting
    on       - Enable TACACS+ authentication
    off      - Disable TACACS+ authentication
    cur      - Display current TACACS+ settings
```

Table 146. TACACS+ Server Menu Options (/cfg/sys/tacacs)

Command Syntax and Usage
`prisrv` *<IP address>* Defines the primary TACACS+ server address.
`secsrv` *<IP address>* Defines the secondary TACACS+ server address.
`chpass_p` Configures the password for the primary TACACS+ server. The CLI will prompt you for input.
`chpass_s` Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.
`secret` *<1-32 character secret>* This is the shared secret between the switch and the TACACS+ server(s).
`secret2` *<1-32 character secret>* This is the secondary shared secret between the switch and the TACACS+ server(s).
`port` *<TACACS port>* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 49.

Table 146. TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

Command Syntax and Usage
`retries` *<TACACS server retries, 1-3>* Sets the number of failed authentication requests before switching to a different TACACS+ server. The default is 3 requests.
`attempts` *<1-10>* Sets the number of failed login attempts before disconnecting the user. The default is 2 attempts.
`timeout` *<TACACS server timeout seconds, 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.
`sloopif` *<1-5>* Sets the TACACS+ source loopback interface.
`usermap` *<0-15>* `user|oper|admin|none` Maps a TACACS+ authorization level to a switch user level. Enter a TACACS+ authorization level (0-15), followed by the corresponding switch user level.
`bckdoor disable|enable` 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 switch, contact your IBM Service and Support line.
`secbd enable|disable` 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 setting is `disabled`.
`cmap enable|disable` Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`.
`passch enable|disable` Enables or disables TACACS+ password change. The default setting is `disabled`.

Table 146. TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

Command Syntax and Usage
`cauth disable|enable` Enables or disables TACACS+ command authorization.
`clog disable|enable` Enables or disables TACACS+ command logging.
`dreq disable|enable` 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.
`acct enable|disable` Enables or disables TACACS+ accounting.
`on` Enables the TACACS+ server. This is the default setting.
`off` Disables the TACACS+ server.
`cur` Displays current TACACS+ configuration parameters.

/cfg/sys/ldap
LDAP Server Configuration Menu

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.

```
[LDAP Server Menu]
     prisrv   - Set IP address of primary LDAP server
     secsrv   - Set IP address of secondary LDAP server
     port     - Set LDAP port number
     retries  - Set number of LDAP server retries
     timeout  - Set timeout value of LDAP server retries
     domain   - Set domain name
     bckdoor  - Enable/disable LDAP backdoor for telnet/ssh/http/https
     on       - Enable LDAP authentication
     off      - Disable LDAP authentication
     cur      - Display current LDAP settings
```

Table 147. LDAP Server Menu Options (/cfg/sys/ldap)

Command Syntax and Usage
`prisrv` *<IP address>* Defines the primary LDAP server address.
`secsrv` *<IP address>* Defines the secondary LDAP server address.
`port` *<LDAP port>* Enter the number of the TCP port to be configured, between 1 - 65000. The default is 389.
`retries` *<LDAP server retries, 1-3>* Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.
`timeout` *<LDAP server timeout seconds, 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.

`domain` *<domain name (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`

`bckdoor disable|enable` 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 switch, contact your Service and Support line.
`on` Enables the LDAP server.
`off` Disables the LDAP server. This is the default setting.
`cur` Displays current LDAP configuration parameters.

/cfg/sys/ntp

NTP Client Configuration Menu

```
[NTP Server Menu]
      prisrv   - Set primary NTP server address
      secsrv   - Set secondary NTP server address
      intrval  - Set NTP server resync interval
      sloopif  - Set NTP source loopback interface
      auth     - Enable/Disable NTP authentication
      md5key   - NTP MD5 Key Menu
      prikey   - Add NTP primary server key
      seckey   - Add NTP secondary server key
      addkey   - Add NTP trusted key
      remkey   - Remove NTP trusted key
      on       - Turn NTP service ON
      off      - Turn NTP service OFF
      cur      - Display current NTP configuration
```

This menu enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

Table 148. NTP Configuration Menu Options (/cfg/sys/ntp)

Command Syntax and Usage
`prisrv` *<IP address>* `[-m|-mgt|-e|-extm|-d|-data]` 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`), or data port (`data`).
`secsrv` *<IP address>* `[-m|-mgt|-e|-extm|-d|-data]` 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`), or data port (`data`).
`intrval` *<5-44640>* Specifies the time interval, in minutes, to re-synchronize the switch clock with the NTP server.
`auth enable|disable` Enables or disables NTP authentication. The default setting is `disabled`. When authentication is enabled, the switch transmits NTP packets with the MAC address appended.
`md5key` *<1-65534>* Displays the MD5 Key configuration menu. To view menu options, see page 210.
`prikey` *<1-65534>* Adds the NTP primary server key, which specifies which MD5 key is used by the primary server.

Table 148. NTP Configuration Menu Options (/cfg/sys/ntp) (continued)

Command Syntax and Usage
`seckey` *<1-65534>* Adds the NTP secondary server key, which specifies which MD5 key is used by the secondary server.
`addkey` *<1-65534>* Adds an MD5 key code to the list of trusted keys.
`remkey` *<1-65534>* Removes the specified key code from the list of trusted keys.
`sloopif` *<1-5>* Sets the NTP source loopback interface.
`on` Enables the NTP synchronization service.
`off` Disables the NTP synchronization service.
`cur` Displays the current NTP service settings.

/cfg/sys/ntp/md5key *<1-65534>*
NTP MD5 Key Menu

```
[NTP MD5 Key 1 Menu]
     key      - Set authentication key
     delete   - Delete key
     cur      - Display current MD5 key configuration
```

Table 149. NTP MD5 KEy Configuration Menu Options (/cfg/sys/ntp/md5key)

Command Syntax and Usage
`key` *<1-16 characters>* Configures the selected MD5 key code.
`delete` Deletes the selected MD5 key code.
`cur` Displays the current NTP MD5 key settings.

/cfg/sys/ssnmp
System SNMP Configuration Menu

```
[System SNMP Menu]
     snmpv3    - SNMPv3 Menu
     name      - Set SNMP "sysName"
     locn      - Set SNMP "sysLocation"
     cont      - Set SNMP "sysContact"
     rcomm     - Set SNMP read community string
     wcomm     - Set SNMP write community string
     trsrc     - Set SNMP trap source interface for SNMPv1
     trloopif - Set SNMP trap source loopback interface
     thostadd - Add a new trap host
     thostrem - Remove an existing trap host
     timeout   - Set timeout for the SNMP state machine
     auth      - Enable/disable SNMP "sysAuthenTrap"
     linkt     - Enable/disable SNMP link up/down trap
     cur       - Display current 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 150. System SNMP Menu Options (/cfg/sys/ssnmp)

Command Syntax and Usage
`snmpv3` Displays SNMPv3 menu. To view menu options, see page 213.
`name` *<1-64 characters>* Configures the name for the system.
`locn` *<1-64 characters>* Configures the name of the system location.

Table 150. System SNMP Menu Options (/cfg/sys/ssnmp) (continued)

Command Syntax and Usage
`cont` *<1-64 characters>* Configures the name of the system contact.
`rcomm` *<1-32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. The default read community string is *public*.
`wcomm` *<1-32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. The default write community string is *private*.
`trsrc` *<interface number>* Configures the source interface for SNMP traps. The default value is interface 1. To send traps through the management ports, specify interface 128.
`trloopif` *<1-5>* Configures the loopback interface for SNMP traps.
`thostadd` *<trap host IP address>* *<trap host community string>* Adds a trap host server.
`thostrem` *<trap host IP address>* Removes the trap host server.
`timeout` *<1-30>* Set the timeout value for the SNMP state machine, in minutes.
`auth disable|enable` Enables or disables the use of the system authentication trap facility. The default setting is `disabled`.
`linkt` *<port>* {`disable|enable`} Enables or disables the sending of SNMP link up and link down traps. The default setting is `enabled`.
`cur` Displays the current SNMP configuration.

/cfg/sys/ssnmp/snmpv3

SNMPv3 Configuration Menu

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.

```
[SNMPv3 Menu]
     usm       - usmUser Table menu
     view      - vacmViewTreeFamily Table menu
     access    - vacmAccess Table menu
     group     - vacmSecurityToGroup Table menu
     comm      - community Table menu
     taddr     - targetAddr Table menu
     tparam    - targetParams Table menu
     notify    - notify Table menu
     v1v2      - Enable/disable V1/V2 access
     cur       - Display current SNMPv3 configuration
```

Table 151. SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

Command Syntax and Usage
`usm` *<usmUser number (1-16)>* Defines a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view menu options, see page 215.
`view` *<vacmViewTreeFamily number (1-128)>* Allows you to create different MIB views. To view menu options, see page 216.
`access` *<vacmAccess number (1-32)>* Configures the access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view menu options, see page 217.
`group` *<vacmSecurityToGroup number (1-16)>* Maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view menu options, see page 218.
`comm` *<snmpCommunity number (1-16)>* The community table contains objects for mapping community strings and version-independent SNMP message parameters. To view menu options, see page 219.

Table 151. SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3) (continued)

`taddr` *<snmpTargetAddr number (1-16)>* Allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view menu options, see page 220.
`tparam` *<target params index (1-16)>* Allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view menu options, see page 221.
`notify` *<notify index (1-16)>* A notification application typically monitors a system for particular events or conditions, and generates Notification-Class messages based on these events or conditions. To view menu options, see page 222.
`v1v2 disable|enable` Allows you to enable or disable the access to SNMP version 1 and version 2. The default setting is `disabled`.
`cur` Displays the current SNMPv3 configuration.

/cfg/sys/ssnmp/snmpv3/usm

User Security Model Configuration Menu

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.

This menu helps you create a user security model entry for an authorized user. You need to provide a security name to create the USM entry.

```
[SNMPv3 usmUser 1 Menu]
     name     - Set USM user name
     auth     - Set authentication protocol
     authpw   - Set authentication password
     priv     - Set privacy protocol
     privpw   - Set privacy password
     del      - Delete usmUser entry
     cur      - Display current usmUser configuration
```

Table 152. User Security Model Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/usm)

Command Syntax and Usage
`name` *<1-32 characters>* Defines a string that represents the name of the user. This is the login name that you need in order to access the switch.
`auth {md5|sha|none}` Configures the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is none.
`authpw` Allows you to create or change your password for authentication. If you selected an authentication algorithm using the above command, you need to provide a password, otherwise you will get an error message during validation.
`priv des|none` Configures the type of privacy protocol on your switch. The privacy protocol protects messages from disclosure. The options are des (CBC-DES Symmetric Encryption Protocol) or none. If you specify des as the privacy protocol, then make sure that you have selected one of the authentication protocols (MD5 or HMAC-SHA-96). If you select none as the authentication protocol, you will get an error message.
`privpw` Defines the privacy password.
`del` Deletes the selected USM user entries.
`cur` Displays the selected USM user entries.

/cfg/sys/ssnmp/snmpv3/view

SNMPv3 View Configuration Menu

```
[SNMPv3 vacmViewTreeFamily 1 Menu]
    name    - Set view name
    tree    - Set MIB subtree(OID) which defines a family of view subtrees
    mask    - Set view mask
    type    - Set view type
    del     - Delete vacmViewTreeFamily entry
    cur     - Display current vacmViewTreeFamily configuration
```

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

Table 153. SNMPv3 View Menu Options (/cfg/sys/ssnmp/snmpv3/view)

Command Syntax and Usage
`name` *<1-32 characters>* Defines the name for a family of view subtrees.
`tree` *<object identifier, such as 1.3.6.1.2.1.1.1.0 (1-64 characters)>* Defines the MIB tree which, when combined with the corresponding mask, defines a family of view subtrees.
`mask` *<bitmask, 1-32 characters>*|`none` Configures the bit mask, which in combination with the corresponding tree, defines a family of view subtrees.
`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.
`del` Deletes the `vacmViewTreeFamily` group entry.
`cur` Displays the current `vacmViewTreeFamily` configuration.

/cfg/sys/ssnmp/snmpv3/access

View-Based Access Control Model Configuration Menu

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.

```
[SNMPv3 vacmAccess 1 Menu]
     name     - Set group name
     prefix   - Set content prefix
     model    - Set security model
     level    - Set minimum level of security
     match    - Set prefix only or exact match
     rview    - Set read view index
     wview    - Set write view index
     nview    - Set notify view index
     del      - Delete vacmAccess entry
     cur      - Display current vacmAccess configuration
```

Table 154. View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage
`name` *<1-32 characters>* Defines the name of the group.
`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.
`model usm|snmpv1|snmpv2` Allows you to select the security model to be used.
`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.
`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.
`rview` *<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.

Table 154. View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access) (continued)

Command Syntax and Usage
`wview` *<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.
`nview` *<1-32 characters>* Defines a long notify view name that allows you notify access to the MIB view.
`del` Deletes the View-based Access Control entry.
`cur` Displays the View-based Access Control configuration.

/cfg/sys/ssnmp/snmpv3/group

SNMPv3 Group Configuration Menu

```
[SNMPv3 vacmSecurityToGroup 1 Menu]
     model    - Set security model
     uname    - Set USM user name
     gname    - Set group gname
     del      - Delete vacmSecurityToGroup entry
     cur      - Display current vacmSecurityToGroup configuration
```

Table 155. SNMPv3 Group Menu Options (/cfg/sys/ssnmp/snmpv3/group)

Command Syntax and Usage
`model usm|snmpv1|snmpv2` Defines the security model.
`uname` *<1-32 characters>* Sets the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 215.
`gname` *<1-32 characters>* The name for the access group as defined in `/cfg/sys/ssnmp/snmpv3/access/name` on page 217.
`del` Deletes the `vacmSecurityToGroup` entry.
`cur` Displays the current `vacmSecurityToGroup` configuration.

/cfg/sys/ssnmp/snmpv3/comm

SNMPv3 Community Table Configuration Menu

This command is 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.

```
[SNMPv3 snmpCommunityTable 1 Menu]
     index    - Set community index
     name     - Set community string
     uname    - Set USM user name
     tag      - Set community tag
     del      - Delete communityTable entry
     cur      - Display current communityTable configuration
```

Table 156. SNMPv3 Community Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/comm)

Command Syntax and Usage
`index` *<1-32 characters>* Configures the unique index value of a row in this table.
`name` *<1-32 characters>* Defines the user name as defined in the `/cfg/sys/ssnmp/snmpv3/usm/name` command.
`uname` *<1-32 characters>* Defines a readable text string that represents the corresponding value of an SNMP community name in a security model.
`tag` *<1-255 characters>* Configures a tag that specifies a set of transport endpoints to which a command responder application sends an SNMP trap.
`del` Deletes the community table entry.
`cur` Displays the community table configuration.

/cfg/sys/ssnmp/snmpv3/taddr

SNMPv3 Target Address Table Configuration Menu

This command is 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.

```
[SNMPv3 snmpTargetAddrTable 1 Menu]
     name     - Set target address name
     addr     - Set target transport address IP
     port     - Set target transport address port
     taglist  - Set tag list
     pname    - Set targetParams name
     del      - Delete targetAddrTable entry
     cur      - Display current targetAddrTable configuration
```

Table 157. Target Address Table Menu Options (/cfg/sys/ssnmp/snmpv3/taddr)

Command Syntax and Usage
`name` *<1-32 characters>* Defines the locally arbitrary, but unique identifier, target address name associated with this entry.
`addr` *<transport IP address>* Configures a transport IPv4 address that can be used in the generation of SNMP traps.
`port` *<transport address port>* Configures a transport address port that can be used in the generation of SNMP traps.
`taglist` *<1-255 characters>* Allows you to configure a list of tags that are used to select target addresses for a particular operation.
`pname` *<1-32 characters>* Defines the name as defined in the `/cfg/sys/ssnmp/snmpv3/tparam/name` command on page 221.
`del` Deletes the Target Address Table entry.
`cur` Displays the current Target Address Table configuration.

/cfg/sys/ssnmp/snmpv3/tparam

SNMPv3 Target Parameters Table Configuration Menu

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).

```
[SNMPv3 snmpTargetParamsTable 1 Menu]
     name      - Set target params name
     mpmodel   - Set message processing model
     model     - Set security model
     uname     - Set USM user name
     level     - Set minimum level of security
     del       - Delete targetParamsTable entry
     cur       - Display current targetParamsTable configuration
```

Table 158. Target Parameters Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/tparam)

Command Syntax and Usage
name *<1-32 characters>* Defines the locally arbitrary, but unique identifier that is associated with this entry.
mpmodel snmpv1|snmpv2c|snmpv3 Configures the message processing model that is used to generate SNMP messages.
model usm|snmpv1|snmpv2 Allows you to select the security model to be used when generating the SNMP messages.
uname *<1-32 characters>* Defines the name that identifies the user in the USM table (page 215) on whose behalf the SNMP messages are generated using this entry.
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.
del Deletes the targetParamsTable entry.
cur Displays the current targetParamsTable configuration.

/cfg/sys/ssnmp/snmpv3/notify

SNMPv3 Notify Table Configuration Menu

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.

```
[SNMPv3 snmpNotifyTable 1  Menu]
     name     - Set notify name
     tag      - Set notify tag
     del      - Delete notifyTable entry
     cur      - Display current notifyTable configuration
```

Table 159. Notify Table Menu Options (/cfg/sys/ssnmp/snmpv3/notify)

Command Syntax and Usage
`name` *<1-32 characters>* Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
`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.
`del` Deletes the notify table entry.
`cur` Displays the current notify table configuration.

/cfg/sys/access

System Access Configuration Menu

```
[System Access Menu]
     mgmt     - Management Network Definition Menu
     user     - User Access Control Menu (passwords)
     https    - HTTPS Web Access Menu
     snmp     - Set SNMP access control
     tnport   - Set Telnet server port number
     tport    - Set the TFTP Port for the system
     wport    - Set HTTP (Web) server port number
     http     - Enable/disable HTTP (Web) access
     tnet     - Enable/disable Telnet access
     tsbbi    - Enable/disable Telnet/SSH configuration from BBI
     userbbi  - Enable/disable user configuration from BBI
     cur      - Display current system access configuration
```

Table 160. System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage
`mgmt` Displays the Management Configuration Menu. To view menu options, see page 224.
`user` Displays the User Access Control Menu. To view menu options, see page 225.
`https` Displays the HTTPS Menu. To view menu options, see page 228.
`snmp {disable|read-only|read-write}` Disables or provides read-only/write-read SNMP access.
`tnport` *<TCP port number>* Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port.
`tport` *<TFTP port number (1-65535)>* Sets the TFTP port for the switch. The default is port 69.
`wport` *<TCP port number (1-65535)>* Sets the switch port used for serving switch Web content. The default is HTTP port 80. If Global Server Load Balancing is to be used, set this to a different port (such as 8080).
`http disable|enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. The default setting is `disabled`.
`tnet enable|disable` Enables or disables Telnet access. The default setting is `disabled`.
`tsbbi enable|disable` Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).

Table 160. System Access Menu Options (/cfg/sys/access) (continued)

Command Syntax and Usage
`userbbi enable|disable` Enables or disables user configuration access through the Browser-Based Interface (BBI).
`cur` Displays the current system access parameters.

/cfg/sys/access/mgmt
Management Networks Configuration Menu

```
[Management Networks Menu]
     add      - Add mgmt network definition
     rem      - Remove mgmt network definition
     cur      - Display current mgmt network definitions
     clear    - Clear current mgmt network definitions
```

This menu is used to define IP address ranges which are allowed to access the switch for management purposes.

Table 161. Management Network Options

Command Syntax and Usage
`add` *<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. You can add up to 10 management networks.
`rem` *<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.
`cur` Displays the current configuration.
`clear` Removes all defined management networks.

/cfg/sys/access/user
User Access Control Configuration Menu

```
[User Access Control Menu]
     uid      - User ID Menu
     eject    - Eject user
     usrpw    - Set user password (user)
     opw      - Set operator password (oper)
     admpw    - Set administrator password (admin)
     strongpw - Strong password menu
     cur      - Display current user status
```

Note: Passwords can be a maximum of 128 characters.

Table 162. User Access Control Menu Options (/cfg/sys/access/user)

Command Syntax and Usage
`uid` *<user ID (1-10)>* Displays the User ID Menu. To view menu options, see page 226.
`eject user|oper|admin|<user name>` Ejects the specified user from the CN4093.
`usrpw` *<1-128 characters>* 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).
`opw` *<1-128 characters>* 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).
`admpw` *<1-128 characters>* Sets the administrator (`admin`) password. The administrator has complete access to all menus, information, and configuration commands on the CN4093, including the ability to change both the user and administrator passwords. This command will prompt for required information: current admin password, new password (up to 128 characters) and confirmation of the new password. Access includes "`oper`" functions. **Note:** You cannot disable the administrator password.

Table 162. User Access Control Menu Options (/cfg/sys/access/user) (continued)

Command Syntax and Usage
`strongpw` Displays the Strong User Password Menu. To view menu options, see page 227.
`cur` Displays the current user status.

/cfg/sys/access/user/uid <1-10>

System User ID Configuration Menu

```
[User ID 1 Menu]
     cos      - Set class of service
     name     - Set user name
     pswd     - Set user password
     ena      - Enable user ID
     dis      - Disable user ID
     del      - Delete user ID
     cur      - Display current user configuration
```

Table 163. User ID Configuration Menu Options (/cfg/sys/access/user/uid)

Command Syntax and Usage
`cos` *<user|oper|admin>* 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.
`name` *<1-8 characters>* Sets the user name (maximum of eight characters).
`pswd` *<1-128 characters>* Sets the user password.
`ena` Enables the user ID.
`dis` Disables the user ID.
`del` Deletes the user ID.
`cur` Displays the current user ID configuration.

/cfg/sys/access/user/strongpw

Strong Password Configuration Menu

```
[Strong Pwd Menu]
     ena      - Enable usage of strong passwords
     dis      - Disable usage of strong passwords
     expiry   - Set password validity
     warning  - Set warning days before pswd expiry
     faillog  - Set number of failed logins for security notification
     cur      - Display current strong password configuration
```

Table 164. Strong Password Menu Options (/cfg/sys/access/user/strongpw)

Command Syntax and Usage
ena Enables Strong Password requirement.
dis Disables Strong Password requirement.
expiry <*1-365*> Configures the number of days allowed before the password must be changed. The default value is 60 days.
warning <*1-365*> Configures the number of days before password expiration, that a warning is issued to users. The default value is 15 days.
faillog <*1-255*> Configures the number of failed login attempts allowed before a security notification is logged. The default value is 3 login attempts.
cur Displays the current Strong Password configuration.

/cfg/sys/access/https
HTTPS Access Configuration

```
[https Menu]
     access   - Enable/Disable HTTPS Web access
     port     - HTTPS WebServer port number
     generate - Generate self-signed HTTPS server certificate
     certSave - save HTTPS certificate
     gtca     - Import ca root certificate via TFTP
     gthkey   - Import host private key via TFTP
     gthcert  - Import host certificate via TFTP
     cur      - Display current SSL Web Access configuration
```

Table 165. HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

Command Syntax and Usage
`access ena|dis` Enables or disables BBI access (Web access) using HTTPS. The default setting is `enabled`.
`port` *<TCP port number>* Defines the HTTPS Web server port number. The default port is 443.
`generate` Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example: – Country Name (2 letter code) []: CA – State or Province Name (full name) []: Ontario – Locality Name (for example, city) []: Ottawa – Organization Name (for example, company) []: IBM – Organizational Unit Name (for example, section) []: Datacenter – Common Name (for example, user's name) []: Mr Smith – Email (for example, email address) []: info@ibm.com You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.
`certSave` Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.
`gtca` {*<hostname>*|*<IP address>*} *<filename>* Enables you to import a Certificate of Authority root certificate using TFTP.
`gthkey` {*<hostname>*|*<IP address>*} *<filename>* Enables you to import a host private key using TFTP.

Table 165. HTTPS Access Configuration Menu Options (/cfg/sys/access/https) (continued)

Command Syntax and Usage
`gthcert {<hostname>|<IP address>} <filename>` Enables you to import a host certificate using TFTP.
`cur` Displays the current SSL Web Access configuration.

/cfg/sys/dst
Custom Daylight Savings Time Configuration Menu

```
[Custom DST Menu]
     dststart - Set the DST start day
     dstend   - Set the DST stop day
     ena      - Enable custom DST
     dis      - Disable custom DST
     cur      - Display custom DST configuration
```

Use this menu to configure custom Daylight Savings Time. The DST will be defined by two rules, the start rule and end rule. The rules specify the date and time 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 166. Custom DST Configuration Menu Options (/cfg/sys/dst)

Command Syntax and Usage

`dststart {<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.

`dstend {<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.

Table 166. Custom DST Configuration Menu Options (/cfg/sys/dst) (continued)

Command Syntax and Usage
ena Enables the Custom Daylight Savings Time settings.
dis Disables the Custom Daylight Savings Time settings.
cur Displays the current Custom DST configuration.

/cfg/sys/sflow
sFlow Configuration Menu

```
[sFlow Menu]
     ena      - Enable sFlow
     dis      - Disable sFlow
     saddress - Set the sFlow Analyzer IP address
     sport    - Set the sFlow Analyzer port
     port     - sFlow port Menu
     cur      - Display sFlow configuration
```

IBM Networking OS supports sFlow version 5. sFlow is a sampling method used for monitoring high speed switched networks. Use this menu to configure the sFlow agent on the switch.

Table 167. sFlow Configuration Menu Options (/cfg/sys/sflow)

Command Syntax and Usage
ena Enables the sFlow agent.
dis Disables the sFlow agent.
saddress *<IP address>* Defines the sFlow server address.
sport *<1-65535>* Configures the UDP port for the sFlow server. The default value is 6343.
port *<port alias or number>* Configures the sFlow interface port.
cur Displays the current sFlow configuration.

/cfg/sys/sflow/port <*port alias or number*>
sFlow Port Configuration Menu

```
[sFlow Port Menu]
     polling  - Set the sFlow polling interval
     sampling - Set the sFlow sampling rate
     cur      - Display sFlow port configuration
```

Use this menu to configure the sFlow port on the switch.

Table 168. sFlow Port Configuration Menu Options (/cfg/sys/sflow/port)

Command Syntax and Usage
polling <*5-60*>|0 Configures the sFlow polling interval, in seconds. The default value is 0 (disabled).
sampling <*256-65536*>|0 Configures the sFlow sampling rate, in packets per sample. The default value is 0 (disabled).
cur Displays the current sFlow port configuration.

/cfg/port <*port alias or number*>
Port Configuration Menu

```
[Port INTA1 Menu]
     gig      - Gig Phy Menu
     udld     - UDLD Menu
     oam      - OAM Menu
     aclqos   - Acl/Qos Configuration Menu
     stp      - STP Menu
     8021ppri - Set default 802.1p priority
     pvid     - Set default port VLAN id
     name     - Set port name
     bpdugrd  - Enable/disable BPDU Guard
     dscpmrk  - Enable/disable DSCP remarking for port
     rmon     - Enable/disable RMON for port
     tag      - Enable/disable VLAN tagging for port
     tagpvid  - Enable/disable tagging on pvid
     floodblk - Enable/disable Port flood blocking
     brate    - Set BroadCast Threshold
     mrate    - Set MultiCast Threshold
     drate    - Set Dest. Lookup Fail Threshold
     evbprof  - Set EVB Port Profile
     ena      - Enable port
     dis      - Disable port
     cur      - Display current port configuration
```

Use the Port Configuration menu to configure settings for internal ports (INTx) and external ports (EXTx). However, if you are configuring management ports (MGT1 or EXTM), see "Management Port Configuration Menu" on page 241.

Table 169. Port Configuration Menu Options (/cfg/port)

Command Syntax and Usage
`errdis` Displays the Error Disable and Recovery menu. To view menu options, see page 234.
`gig` If a port is configured to support Gigabit Ethernet, this option displays the Gigabit Ethernet Physical Link Menu. To view menu options, see page 236.
`udld` Displays the Unidirectional Link Detection (UDLD) Menu. To view menu options, see page 237.
`oam` Displays the OAM Discovery Configuration Menu. To view menu options, see page 238.
`aclqos` Displays the ACL/QoS Configuration Menu. To view menu options, see page 239.
`stp` Displays the Spanning Tree Port menu. To view menu options, see page 239.

Table 169. Port Configuration Menu Options (/cfg/port) (continued)

Command Syntax and Usage
`8021ppri` *<0-7>* Configures the port's 802.1p priority level.
`pvid` *<VLAN number>* Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1 for non-management ports.
`name` *<1-64 characters>*`|none` Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens. The default setting is `none`.
`bpdugrd e|d` Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.
`dscpmark` Enables or disables DSCP re-marking on a port.
`rmon e|d` Enables or disables Remote Monitoring for the port. RMON must be enabled for any RMON configurations to function.
`tag disable|enable` Disables or enables VLAN tagging for this port. The default setting is `disabled` for external ports (EXTx) and `enabled` for internal server ports (INTx).
`tagpvid disable|enable` Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default setting is `disabled` for external (EXTx) ports and internal server ports (INTx), and `enabled` for MGT ports.
`floodblk disable|enable` Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.
`brate` *<0-262143>*`|dis` Limits the number of broadcast packets per second to the specified value. If disabled (`dis`), the port forwards all broadcast packets.
`mrate` *<0-262143>*`|dis` Limits the number of multicast packets per second to the specified value. If disabled (`dis`), the port forwards all multicast packets.
`drate` *<0-262143>*`|dis` Limits the number of unknown unicast packets per second to the specified value. If disabled (`dis`), the port forwards all unknown unicast packets.
`evbprof` *<0-16>* Adds the specified Edge Virtual Bridge (EVB) profile to the port.

Table 169. Port Configuration Menu Options (/cfg/port) (continued)

Command Syntax and Usage
`ena` Enables the port.
`dis` Disables the port. (To temporarily disable a port without changing its configuration attributes, refer to "Temporarily Disabling a Port" on page 234.)
`cur` Displays current port parameters.

Temporarily Disabling a Port

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

```
Main# /oper/port <port alias or number>/dis
```

Because this configuration sets a temporary state for the port, you do not need to use `apply` or `save`. The port state will revert to its original configuration when the CN4093 is reset. See the "Operations Menu" on page 433 for other operations-level commands.

/cfg/port <port alias or number>/errdis
Port Error Disable and Recovery Configuration

```
[Port 2 ErrDisable Menu]
     lfd      - Link Flap Dampening Menu
     ena      - Enable ErrDisable recovery
     dis      - Disable ErrDisable recovery
     cur      - Display current ErrDisable 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 170. Port Error Disable Configuration Options

Command Syntax and Usage
`lfd` Displays the Link Flap Dampening menu. To view menu options, see page 234.
`ena` 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 (`/cfg/sys/errdis/ena`).

Table 170. Port Error Disable Configuration Options

Command Syntax and Usage
`dis` Disables automatic error-recovery for the port.
`cur` Displays current port Error Disable parameters.

/cfg/port <*port alias or number*>/errdis/lfd

Link Flap Dampening Menu

```
[Port INTA1 Link Flap Dampening Menu]
     ena      - Enable Link Flap Dampening
     dis      - Disable Link Flap Dampening
     cur      - Display current Link Flap Dampening configuration
```

The following table describes the link flap dampening options.

Table 171. Link Flap Dampening Options

Command Syntax and Usage
`ena` Enables link flap dampening.
`dis` Disables link flap dampening.
`cur` Displays the current Link Flap Dampening configuration.

/cfg/port <*port alias or number*>/gig
Port Link Configuration Menu

```
[Gigabit Link Menu]
     speed    - Set link speed
     mode     - Set full or half duplex mode
     fctl     - Set flow control
     auto     - Set autonegotiation
     cur      - Display current gig link configuration
```

Link menu options are described in the following table.

Table 172. Port Link Configuration Menu Options (/cfg/port/gig)

Command Syntax and Usage
`speed 10|100|1000|10000|any` Sets the link speed. Some options are not valid on all ports. The choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – 10000 Mbps – any (auto negotiate port speed) **Note**: External 1/10Gb port speed becomes fixed when a transceiver is plugged into the port.
`mode full|half|any` Sets the operating mode. Some options are not valid on all ports. The choices include: – Full-duplex – Half-duplex – “Any,” for auto negotiation (default)
`fctl rx|tx|both|none` Sets the flow control. The choices include: – Receive flow control – Transmit flow control – Both receive and transmit flow control – No flow control **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.
`auto on|off` Turns auto-negotiation on or off.
`cur` Displays current port parameters.

/cfg/port <*port alias or number*>/udld
UniDirectional Link Detection Configuration Menu

```
[UDLD Menu]
     mode     - Set UDLD mode
     ena      - Enable UDLD
     dis      - Disable UDLD
     cur      - Display current port UDLD configuration
```

UDLD menu options are described in the following table.

Table 173. Port UDLD Configuration Menu Options (/cfg/port/udld)

Command Syntax and Usage
`mode normal|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. – **Aggressive**: In addition to the normal mode, the aggressive mode disables the port if the neighbor stops sending UDLD probes for 7 seconds.
`ena` Enables UDLD on the port.
`dis` Disables UDLD on the port.
`cur` Displays current port UDLD parameters.

/cfg/port <*port alias or number*>/oam
Port OAM Configuration Menu

```
[OAM Menu]
     ena       - Enable OAM Discovery process
     dis       - Disable OAM Discovery process
     mode      - Set OAM mode
     cur       - Display current 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 menu options are described in the following table.

Table 174. Port OAM Configuration Menu Options (/cfg/port/oam)

Command Syntax and Usage
ena Enables OAM discovery on the port.
dis Disables OAM discovery on the port.
mode active|passive Configures the OAM discovery mode, as follows: – Active: This port link initiates OAM discovery. – 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.
cur Displays current port OAM parameters.

/cfg/port <*port alias or number*>/aclqos
Port ACL Configuration Menu

```
[Port INT2 ACL Menu]
     add      - Add ACL or ACL group to this port
     rem      - Remove ACL or ACL group from this port
     cur      - Display current ACLs for this port
```

Table 175. Port ACL Menu Options (/cfg/port/aclqos)

Command Syntax and Usage
`add acl|acl6|grp` <*ACL or ACL group number*> Adds the specified ACL or ACL group to the port. You can add multiple ACL groups to a port.
`rem acl|acl6|grp` <*ACL or ACL group number*> Removes the specified ACL or ACL group from the port.
`cur` Displays current ACL QoS parameters.

/cfg/port <*port alias or number*>/stp
Port Spanning Tree Configuration Menu

```
[Port INTA1 STP Menu]
    edge   - Enable/disable edge port (for PVRST only)
    link   - Set port link type (auto, p2p, or shared; default: auto)
    guard  - Set Port Guard Type Menu
    cur    - Display current port stp configuration
```

Table 176. Port STP Menu Options (/cfg/port/stp)

Command Syntax and Usage
`edge e|d` Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (`enabled`). **Note**: After you configure the port as an edge port, you must disable the port (`/oper/port` *x*`/dis`) and then re-enable the port (`/oper/port` *x*`/ena`) for the change to take effect.
`link auto|p2p|shared` Defines the type of link connected to the port, as follows: – `auto`: Configures the port to detect the link type, and automatically match its settings. – `p2p`: Configures the port for Point-To-Point protocol. – `shared`: Configures the port to connect to a shared medium (usually a hub). The default link type is `auto`.

Table 176. Port STP Menu Options (/cfg/port/stp) (continued)

Command Syntax and Usage
`guard` Displays the Spanning Tree Guard menu for the port. To view menu options, see page 241.
`cur` Displays current STP parameters for the port.

/cfg/port <*port alias or number*>/stp/guard

Port Spanning Tree Guard Configuration

```
[Guard Menu]
     default  - Set guard type to default
     type     - Set guard type
     cur      - Display current guard type
```

Table 177. Port STP Guard Options

Command Syntax and Usage
default Sets the Spanning Tree guard parameters to their default values.
type loop|root|none Defines the Spanning Tree guard type, as follows: – loop: STP loop guard prevents the port from forwarding traffic if no BPDUs are received. The port is placed into a loop-inconsistent blocking state until a BPDU is received. – root: STP root guard enforces the position of the root bridge. If the bridge receives a superior BPDU, the port is placed into a root-inconsistent state (listening). – none: Disables STP loop guard and root guard.
cur Displays current Spanning Tree guard parameters for the port.

/cfg/port MGT1|EXTM

Management Port Configuration Menu

```
[Gigabit Link Menu]
     speed    - Set link speed
     mode     - Set full or half duplex mode
     fctl     - Set flow control
     ena      - Enable management port
     dis      - Disable management port
     cur      - Display current configuration
```

Use these menu options to set port parameters for management ports. Use this menu to set port parameters for the port link. For MGT1 and EXTM, the values for

speed, duplex, and flow control are fixed, and cannot be configured.

Table 178. Management Port Configuration Menu Options (/cfg/port x)

Command Syntax and Usage
`speed 10|100|1000|any` Sets the link speed. The choices include: – Any — for automatic detection (default) – 10 Mbps – 100 Mbps – 1000 Mbps
`mode full|half|any` Sets the operating mode. The choices include: – Any — used for auto negotiation (default) – Full-duplex – Half-duplex
`fctl rx|tx|both|none` Sets the flow control. The choices include: – Receive flow control – Transmit flow control – Both receive and transmit flow control (default) – No flow control
`ena` Enables the port.
`dis` Disables the port.
`cur` Displays current port parameters.

/cfg/qos
Quality of Service Configuration Menu

```
[QOS Menu]
     8021p    - 802.1p Menu
     dscp     - Dscp Menu
     cur      - Display current QOS configuration
```

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

Table 179. Quality of Service Menu Options (/cfg/qos)

Command Syntax and Usage
`8021p` Displays 802.1p configuration menu. To view menu options, see page 243.
`dscp` Displays DSCP configuration menu. To view menu options, see page 244.
`cur` Displays QoS configuration parameters.

/cfg/qos/8021p
802.1p Configuration Menu

```
[802.1p Menu]
     priq     - Set priority to COS queue mapping
     qweight  - Set weight to a COS queue
     cur      - Display current 802.1p configuration
```

This feature provides the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 180. 802.1p Menu Options (/cfg/qos/8021p)

Command Syntax and Usage
`priq` *<priority (0-7)> <COSq number>* Maps the 802.1p priority to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the COSq that handles the matching traffic. The valid range of the COSq number is set using the `numcos` command.

Table 180. 802.1p Menu Options (/cfg/qos/8021p) (continued)

Command Syntax and Usage
qweight *<COSq number> <weight (0-15)>* Configures the weight of the selected COSq. Enter the COSq number, followed by the scheduling weight (0-15)..
cur Displays the current 802.1p parameters.

/cfg/qos/dscp
DSCP Configuration Menu

```
[dscp Menu]
     dscp     - Remark DSCP value to a new DSCP value
     prio     - Remark DSCP value to a 802.1p priority
     on       - Globally turn DSCP remarking ON
     off      - Globally turn DSCP remarking OFF
     cur      - Display current DSCP remarking configuration
```

Use this menu map the DiffServ Code Point (DSCP) value of incoming packets to a new value, or to an 802.1p priority value.

Table 181. DSCP Menu Options (/cfg/qos/dscp)

Command Syntax and Usage
dscp *<DSCP (0-63)> <new DSCP (0-63)>* Maps the initial DiffServ Code Point (DSCP) value to a new value. Enter the DSCP value (0-63) of incoming packets, followed by the new value.
prio *<DSCP (0-63)> <priority (0-7)>* Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.
on Turns on DSCP re-marking globally.
off Turns off DSCP re-marking globally.
cur Displays the current DSCP parameters.

/cfg/acl

Access Control List Configuration Menu

```
[ACL Menu]
     acl      - Access Control List Item Config Menu
     acl6     - IPv6 Access Control List Item Config Menu
     group    - Access Control List Group Config Menu
     macl     - Management ACL Config Menu
     vmap     - Vlan Map Config Menu
     cur      - Display current ACL configuration
```

Use this menu to create Access Control Lists (ACLs) 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 Menu" on page 239.

Table 182. ACL Menu Options (/cfg/acl)

Command Syntax and Usage
`acl` *<1-256>* Displays Access Control List configuration menu. To view menu options, see page 246.
`acl6` *<1-128>* Displays Access Control List configuration menu. To view menu options, see page 255.
`group` *<1-256>* Displays ACL group configuration menu. To view menu options, see page 261.
`macl` *<1-128>* Displays the Management ACL configuration menu. To view menu options, see page 262.
`vmap` *<1-128>* Displays ACL VLAN Map configuration menu. To view menu options, see page 264.
`cur` Displays the current ACL parameters.

/cfg/acl/acl <*ACL number*>
ACL Configuration Menu

```
[ACL 1 Menu]
     ethernet - Ethernet Header Options Menu
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     pktfmt   - Set to filter specific packet format types
     egrport  - Set to filter for packets egressing this port
     action   - Set filter action
     stats    - Enable/disable statistics for this acl
     reset    - Reset filtering parameters
     cur      - Display current filter configuration
```

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

Table 183. ACL Menu Options (/cfg/acl/acl x)

Command Syntax and Usage
`ethernet` Displays the ACL Ethernet Header menu. To view menu options, see page 247.
`ipv4` Displays the ACL IP Header menu. To view menu options, see page 248.
`tcpudp` Displays the ACL TCP/UDP Header menu. To view menu options, see page 249.
`pktfmt` *<packet format>* Displays the ACL Packet Format menu. To view menu options, see page 254.
`egrport` *<port alias or number>* Configures the ACL to function on egress packets.
`action permit|deny|setprio` *<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).
`stats e|d` Enables or disables the statistics collection for the Access Control List.
`reset` Resets the ACL parameters to their default values.
`cur` Displays the current ACL parameters.

/cfg/acl/acl <*ACL number*>/ethernet
Ethernet Filtering Configuration Menu

```
     smac     - Set to filter on source MAC
     dmac     - Set to filter on destination MAC
     vlan     - Set to filter on VLAN ID
     etype    - Set to filter on ethernet type
     pri      - Set to filter on priority
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define Ethernet matching criteria for an ACL.

Table 184. Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage
`smac` *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the source MAC address for this ACL.
`dmac` *<MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>* Defines the destination MAC address for this ACL.
`vlan` *<VLAN number> <VLAN mask (0xfff)>* Defines a VLAN number and mask for this ACL.
`etype [ARP|IP|IPv6|MPLS|RARP|any|none|`<*other (0x600-0xFFFF)*>`]` Defines the Ethernet type for this ACL.
`pri` *<0-7>* Defines the Ethernet priority value for the ACL.
`reset` Resets Ethernet parameters for the ACL to their default values.
`cur` Displays the current Ethernet parameters for the ACL.

/cfg/acl/acl <*ACL number*>/ipv4
IPv4 Filtering Configuration Menu

```
[Filtering IPv4 Menu]
     sip      - Set to filter on source IP address
     dip      - Set to filter on destination IP address
     proto    - Set to filter on prototype
     tos      - Set to filter on TOS
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define IP version 4 matching criteria for an ACL.

Table 185. IPv4 Filtering Menu Options (/cfg/acl/acl x/ipv4)

Command Syntax and Usage
`sip` *<IP address> <mask (such as 255.255.255.0)>* 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.
`dip` *<IP address> <mask (such as 255.255.255.0)>* Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.
`proto` *<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
`tos` *<0-255>* Defines a Type of Service (ToS) value for the ACL. For more information on ToS, refer to RFC 1340 and 1349.
`reset` Resets the IPv4 parameters for the ACL to their default values.
`cur` Displays the current IPv4 parameters.

/cfg/acl/acl <*ACL number*>/tcpudp
TCP/UDP Filtering Configuration Menu

```
[Filtering TCP/UDP Menu]
     sport    - Set to filter on TCP/UDP source port
     dport    - Set to filter on TCP/UDP destination port
     flags    - Set to filter TCP/UDP flags
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 186. TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage
`sport` *<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
`dport` *<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.
`flags` *<value (0x0-0x3f)> <mask (0x0-0x3f)>* Defines a TCP/UDP flag for the ACL.
`reset` Resets the TCP/UDP parameters for the ACL to their default values.
`cur` Displays the current TCP/UDP Filtering parameters.

/cfg/acl/acl <*ACL number*>/meter
ACL Metering Configuration Menu

```
[Metering Menu]
     cir      - Set committed rate in kilobits per second
     mbsize   - Set maximum burst size in kilobits
     enable   - Enable/disable port metering
     dpass    - Set to Drop or Pass out of profile traffic
     reset    - Reset meter parameters
     cur      - Display current settings
```

This menu defines the metering profile for the selected ACL.

Table 187. ACL Metering Menu Options (/cfg/acl/acl x/meter)

Command Syntax and Usage
`cir` <*64-40000000*> Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.
`mbsize` <*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
`enable e|d` Enables or disables metering on the ACL.
`dpass drop|pass` Configures the ACL meter to either drop or pass out-of-profile traffic.
`reset` Reset ACL metering parameters to their default values.
`cur` Displays current ACL metering parameters.

/cfg/acl/acl <*ACL number*>/re-mark
Re-Mark Configuration Menu

```
[Re-mark Menu]
     inprof   - In Profile Menu
     outprof  - Out Profile Menu
     up1p     - Set Update User Priority Menu
     reset    - Reset re-mark settings
     cur      - Display current settings
```

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

Table 188. ACL Re-Mark Menu Options (/cfg/acl/acl x/re-mark)

Command Syntax and Usage
`inprof` Displays the Re-Mark In-Profile menu. To view menu options, see page 252.
`outprof` Displays the Re-Mark Out-of-Profile menu. To view menu options, see page 253.
`up1p` Displays the Re-Mark Update User Priority menu. To view menu options, see page 252.
`reset` Reset ACL re-mark parameters to their default values.
`cur` Displays current re-mark parameters.

/cfg/acl/acl <*ACL number*>/re-mark/inprof

Re-Marking In-Profile Configuration Menu

```
[Re-marking - In Profile Menu]
     up1p     - Set Update User Priority Menu
     updscp   - Set the update DSCP
     reset    - Reset update DSCP settings
     cur      - Display current settings
```

Table 189. ACL Re-Mark In-Profile Menu (/cfg/acl/acl x/re-mark/inprof)

Command Syntax and Usage
up1p Displays the Re-Mark Update User Priority menu. To view menu options, see page 252.
updscp <*0-63*> Re-marks the DiffServ Code Point (DSCP) of in-profile packets to the selected value.
reset Resets the re-mark parameters for in-profile packets to their default values.
cur Displays current re-mark in-profile parameters.

/cfg/acl/acl <*ACL number*>/re-mark/up1p

Update User Priority Configuration

```
[Update User Priority Menu]
     value    - Set the update user priority
     utosp    - Enable/Disable use of TOS precedence
     reset    - Reset in profile up1p settings
     cur      - Display current settings
```

Table 190. ACL Re-Mark Update User Priority Options

Command Syntax and Usage
value <*0-7*> Re-marks the 802.1p value. The value is the priority bits information in the packet structure.
utosp enable|disable 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.

Table 190. ACL Re-Mark Update User Priority Options

Command Syntax and Usage
`reset` Resets UP1P settings to their default values.
`cur` Displays current re-mark User Priority parameters for in-profile packets.

/cfg/acl/acl <*ACL number*>/re-mark/outprof
Re-Marking Out-of-Profile Configuration Menu

```
[Re-marking - Out Of Profile Menu]
     updscp   - Set the update DSCP
     reset    - reset update DSCP setting
     cur      - Display current settings
```

Table 191. ACL Re-Mark Out-of-Profile Menu (/cfg/acl/acl x/re-mark/outprof)

Command Syntax and Usage
`updscp` <*0-63*> Re-marks the DiffServ Code Point (DSCP) for out-of-profile packets to the selected value. The switch sets the DSCP value on out-of-profile packets.
`reset` Resets the update DSCP parameters for out-of-profile packets to their default values.
`cur` Displays current re-mark parameters for out-of-profile packets.

/cfg/acl/acl <*ACL number*>/pktfmt
Packet Format Filtering Configuration Menu

```
[Filtering Packet Format Menu]
     ethfmt   - Set to filter on ethernet format
     tagfmt   - Set to filter on ethernet tagging format
     ipfmt    - Set to filter on IP format
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define Packet Format matching criteria for an ACL.

Table 192. ACL Packet Format Filtering Menu Options (/cfg/acl/acl x/pktfmt)

Command Syntax and Usage
`ethfmt {none|eth2|SNAP|LLC}` Defines the Ethernet format for the ACL.
`tagfmt {disabled|any|none|tagged}` Defines the tagging format for the ACL.
`ipfmt {none|v4|v6}` Defines the IP format for the ACL.
`reset` Resets Packet Format parameters for the ACL to their default values.
`cur` Displays the current Packet Format parameters for the ACL.

/cfg/acl/acl6 <*ACL number*>

ACL IPv6 Configuration

```
[ACL6 2 Menu]
     ipv6      - IPv6 Header Options Menu
     tcpudp    - TCP/UDP Header Options Menu
     re-mark   - ACL Re-mark Configuration Menu
     egrport   - Set to filter for packets egressing this port
     action    - Set filter action
     stats     - Enable/disable statistics
     reset     - Reset filtering parameters
     cur       - Display current filter configuration
```

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

Table 193. IPv6 ACL Options

Command Syntax and Usage
`ipv6` Displays the ACL IP Header menu. To view menu options, see page 256.
`tcpudp` Displays the ACL TCP/UDP Header menu. To view menu options, see page 257.
`re-mark` Displays the ACL Re-Mark menu. To view menu options, see page 258.
`egrport` *<port alias or number>* Configures the ACL to function on egress packets.
`action permit|deny|setprio` *<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).
`stats e|d` Enables or disables the statistics collection for the Access Control List.
`reset` Resets the ACL parameters to their default values.
`cur` Displays the current ACL parameters.

/cfg/acl/acl6 <*ACL number*>/ipv6
IP version 6 Filtering Configuration

```
[Filtering IPv6 Menu]
     sip      - Set to filter on source IPv6 address
     dip      - Set to filter on destination IPv6 address
     nexthd   - Set to filter on IPv6 next header
     flabel   - Set to filter on IPv6 flow label
     tclass   - Set to filter on IPv6 traffic class
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define IPv6 matching criteria for an ACL.

Table 194. IP version 6 Filtering Options

Command Syntax and Usage
`sip` *<IPv6 address> <prefix length>* Defines a source IPv6 address for the ACL. If defined, traffic with this source IP address will match this ACL.
`dip` *<IPv6 address> <prefix length>* Defines a destination IPv6 address for the ACL. If defined, traffic with this destination IP address will match this ACL.
`nexthd` *<0-255>* Defines the next header value for the ACL. If defined, traffic with this next header value will match this ACL.
`flabel` *<0-1048575>* Defines the flow label for the ACL. If defined, traffic with this flow label will match this ACL.
`tclass` *<0-255>* Defines the traffic class for the ACL. If defined, traffic with this traffic class will match this ACL.
`reset` Resets the IPv6 parameters for the ACL to their default values.
`cur` Displays the current IPv6 parameters.

/cfg/acl/acl6 <*ACL number*>/tcpudp
IPv6 TCP/UDP Filtering Configuration

```
[Filtering TCP/UDP Menu]
     sport    - Set to filter on TCP/UDP source port
     dport    - Set to filter on TCP/UDP destination port
     flags    - Set to filter TCP/UDP flags
     reset    - Reset all fields
     cur      - Display current parameters
```

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 195. IPv6 ACL TCP/UDP Filtering Options

Command Syntax and Usage
`sport` *<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
`dport` *<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.
`flags` *<value (0x0-0x3f)> <mask (0x0-0x3f)>* Defines a TCP/UDP flag for the ACL.
`reset` Resets the TCP/UDP parameters for the ACL to their default values.
`cur` Displays the current TCP/UDP Filtering parameters.

/cfg/acl/acl6 <*ACL number*>/re-mark

IPv6 Re-Mark Configuration

```
[Re-mark Menu]
     inprof   - In Profile Menu
     up1p     - Set Update User Priority Menu
     reset    - Reset re-mark settings
     cur      - Display current settings
```

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

Table 196. IPv6 ACL Re-Mark Options

Command Syntax and Usage
`inprof` Displays the Re-Mark In-Profile menu. To view menu options, see page 252.
`up1p` Displays the Update User Priority menu. To view menu options, see page 252.
`reset` Reset ACL re-mark parameters to their default values.
`cur` Displays current re-mark parameters.

/cfg/acl/acl6 <*ACL number*>/re-mark/up1p

IPv6 Re-Marking User Priority Configuration

```
[Update User Priority Menu]
     value    - Set the update user priority
     utosp    - Enable/Disable use of TOS precedence
     reset    - Reset in profile up1p settings
     cur      - Display current settings
```

Table 197. IPv6 ACL Update User Priority Options

Command Syntax and Usage
`value` <*0-7*> Re-marks the 802.1p value. The value is the priority bits information in the packet structure.
`utosp enable|disable` 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.
`reset` Resets UP1P settings to their default values.
`cur` Displays current re-mark User Priority parameters for in-profile packets.

/cfg/acl/acl6 <*ACL number*>/re-mark/inprof

IPv6 Re-Marking In-Profile Configuration

```
[Re-marking - In Profile Menu]
     up1p     - Set Update User Priority Menu
     updscp   - Set the update DSCP
     reset    - Reset update DSCP settings
     cur      - Display current settings
```

Table 198. IPv6 ACL Re-mark In-Profile Options

Command Syntax and Usage
`up1p` Displays the Re-Mark Update User Priority menu. To view menu options, see page 260.
`updscp` <*0-63*> Re-marks the DiffServ Code Point (DSCP) of in-profile packets to the selected value.

Table 198. IPv6 ACL Re-mark In-Profile Options

Command Syntax and Usage
`reset` Resets the update DSCP parameters to their default values.
`cur` Displays current re-mark parameters for in-profile packets.

/cfg/acl/acl6 <*ACL number*>/re-mark/inprof/up1p

Update User Priority Configuration

```
[Update User Priority Menu]
     value    - Set the update user priority
     utosp    - Enable/Disable use of TOS precedence
     reset    - Reset in profile up1p settings
     cur      - Display current settings
```

Table 199. ACL Re-Mark Update User Priority Options

Command Syntax and Usage
`value` <*0-7*> Re-marks the 802.1p value. The value is the priority bits information in the packet structure.
`utosp enable|disable` 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.
`reset` Resets UP1P settings to their default values.
`cur` Displays current re-mark User Priority parameters for in-profile packets.

/cfg/acl/group <*ACL group number*>
ACL Group Configuration Menu

```
[ACL Group 1 Menu]
     add      - Add ACL to group
     rem      - Remove ACL from group
     cur      - Display current ACL items in ACL group
```

This menu allows 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 200. ACL Group Menu Options (/cfg/acl/group x)

Command Syntax and Usage
`add acl` *<1-256>* Adds the selected ACL to the ACL group.
`rem acl` *<1-256>* Removes the selected ACL from the ACL group.
`cur` Displays the current ACL group parameters.

/cfg/acl/macl <1-128>
MACL Configuration

```
[MACL 1 Menu]
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     action   - Set filter action
     stats    - Enable/disable statistics
     reset    - Reset filtering parameters
     ena      - Enable the MACL
     dis      - Disable the MACL
     cur      - Display current filter configuration
```

Table 201. Management ACL Configuration Menu Options (/cfg/acl/macl)

Command Syntax and Usage
`ipv4` Displays the IP Header Options menu. To view menu options, see page 262.
`tcpudp` Displays the TCP/UDP Header Options menu. To view menu options, see page 263.
`action` Sets the filter action.
`stats enable|disable` Enables/Disables statistics.
`reset` Resets filtering parameters.
`ena` Enables the MACL.
`dis` Disables the MACL.
`cur` Displays the current filter configuration.

/cfg/acl/macl <1-128>/ipv4
MACL IP Header Configuration

```
[Filtering IPv4 Menu]
     sip      - Set to filter on source IP address
     dip      - Set to filter on destination IP address
     proto    - Set to filter on protocol
     reset    - Reset all fields
     cur      - Display current parameters
```

The following options are available for configuring MACL IP headers.

Table 202. MACL IP Header Configuration Parameters (/cfg/acl/macl/ipv4)

Command Syntax and Usage
`sip` *<source IP address> <address mask>* | `reset` Sets IPv4 filtering to filter on source IP address.
`dip` *<destination IP address> <address mask>* | `reset` Sets IPv4 filtering to filter on destination IP address.
`proto` *<0-255>* Defines an IP protocol for the MACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed here are some of the well-known protocols. **Number Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp
`reset` Resets all fields.
`cur` Displays the current settings.

/cfg/acl/macl *<1-128>*/tcpudp

TCP/UDP Header Configuration

```
[Filtering TCP/UDP Menu]
     sport    - Set to filter on TCP/UDP source port
     dport    - Set to filter on TCP/UDP destination port
     reset    - Reset all fields
     cur      - Display current parameters
```

The following options are available for configuring TCP/UDP headers.

Table 203. TCP/UDP Header Configuration Parameters (/cfg/acl/macl/tcpudp)

Command Syntax and Usage
`sport` *<port number> <address mask>* | `reset` Sets IPv4 filtering to filter on TCP/UDP source port.
`dport` *<port number> <address mask>* | `reset` Sets IPv4 filtering to filter on TCP/UDP destination port.

Table 203. TCP/UDP Header Configuration Parameters (/cfg/acl/macl/tcpudp) (continued)

Command Syntax and Usage
`reset` Resets all fields.
`cur` Displays the current parameters.

/cfg/acl/vmap <1-128>
VMAP Configuration

```
[VMAP 1 Menu]
     mirror   - Mirror Options Menu
     ethernet - Ethernet Header Options Menu
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     meter    - ACL Metering Configuration Menu
     re-mark  - ACL Re-mark Configuration Menu
     pktfmt   - Set to filter specific packet format types
     egrport  - Set to filter for packets egressing this port
     action   - Set filter action
     stats    - Enable/disable statistics
     reset    - Reset filtering parameters
     cur      - Display current filter 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 Menu" on page 245.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration Menu" on page 305.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 424.

/cfg/pmirr
Port Mirroring Configuration

```
[Port Mirroring Menu]
      monport - Monitoring Port based PM Menu
      mirror  - Enable/Disable Mirroring
      cur     - Display All Mirrored and Monitoring Ports
```

Port mirroring is disabled by default. For more information about port mirroring on the CN4093, see "Appendix A: Troubleshooting" in the *IBM Networking OS Application Guide*.

Note: Traffic on VLAN 4095 is not mirrored to the external ports.

The Port Mirroring Menu is used to configure, enable, and disable the monitor port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

Table 204. Port Mirroring Menu Options (/cfg/pmirr)

Command Syntax and Usage
`monport` *<port alias or number>* Displays port-mirroring menu. To view menu options, see page 265.
`mirror disable|enable` Enables or disables port mirroring
`cur` Displays current settings of the mirrored and monitoring ports.

/cfg/pmirr/monport *<port alias or number>*
Port-Mirroring Configuration Menu

```
[Port EXT1 Menu]
     add      - Add "Mirrored" port
     rem      - Rem "Mirrored" port
     delete   - Delete this "Monitor" port
     cur      - Display current Port-based Port Mirroring configuration
```

Table 205. Port Mirroring Monitor Port Menu Options (/cfg/pmirr/monport)

Command Syntax and Usage
`add` *<mirrored port (port to mirror from)> <direction (in, out, or both)>* Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because: If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the monitoring port. If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.
`rem` *<mirrored port (port to mirror from)>* Removes the mirrored port.
`delete` Deletes this monitor port.
`cur` Displays the current settings of the monitoring port.

/cfg/l2

Layer 2 Configuration Menu

```
[Layer 2 Menu]
     8021x    - 802.1x Menu
     mrst     - Multiple Spanning Tree/Rapid Spanning Tree Menu
     nostp    - Disable Spanning Tree
     stg      - Spanning Tree Menu
     fdb      - FDB Menu
     ecp      - ECP Menu
     lldp     - LLDP Menu
     trunk    - Trunk Group Menu
     thash    - Trunk Hash Menu
     vlag     - Virtual Link Aggregation Control Protocol Menu
     lacp     - Link Aggregation Control Protocol Menu
     failovr  - Failover Menu
     hotlink  - Hot Links Menu
     vlan     - VLAN Menu
     vlanstg  - Enable/disable VLAN auto assign STG
     pvstcomp - Enable/disable PVST+ compatibility mode
     loopgrd  - Enable/disable Spanning Tree Loop Guard
     macnotif - Enable/disable MAC address notification
     cur      - Display current layer 2 parameters
```

Table 206. Layer 2 Configuration Menu (/cfg/l2)

Command Syntax and Usage
`8021x` Displays the 802.1X Configuration Menu. To view menu options, see page 268.
`mrst` Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu. To view menu options, see page 274.
`nostp enable|disable` When enabled, globally turns Spanning Tree `off`. All ports are placed into forwarding state. Any BPDU's received are flooded. BPDU Guard is not affected by this command.
`stg` *<group number (1-128)>* Displays the Spanning Tree Configuration Menu. To view menu options, see page 278.
`fdb` Displays the Forwarding Database Menu. To view menu options, see page 282.
`ecp` Displays the Edge Control Protocol menu. To view menu options, see page 284.
`lldp` Displays the LLDP Menu. To view menu options, see page 285.

Table 206. Layer 2 Configuration Menu (/cfg/l2) (continued)

Command Syntax and Usage
`trunk` *<trunk number>* Displays the Trunk Group Configuration Menu. To view menu options, see page 288.
`thash` Displays the Trunk Hash Menu. To view menu options, see page 289.
`vlag` Displays the Virtual Link Aggregation Control Protocol (vLAG) menu. To view menu options, see page 292.
`lacp` Displays the Link Aggregation Control Protocol Menu. To view menu options, see page 295.
`failovr` Displays the Failover Configuration Menu. To view menu options, see page 297.
`hotlink` Displays the Hot Links Configuration menu. To view menu options, see page 302.
`vlan` *<VLAN number (1-4095)>* Displays the VLAN Configuration Menu. To view menu options, see page 305.
`vlanstg enable|disable` Enables or disables VLAN Automatic STG Assignment (VASA). When enabled, each time a new VLAN is configured, the switch will automatically assign the new VLAN its own STG. Conversely, when a VLAN is deleted, if its STG is not associated with any other VLAN, the STG is returned to the available pool. **Note**: VASA applies only to PVRST mode.
`pvstcomp enable|disable` Enables or disables VLAN tagging of Spanning Tree BPDUs. The default setting is `enabled`.
`loopgrd enable|disable` Enables or disables Spanning Tree Loop Guard.
`cur` Displays current Layer 2 parameters.

/cfg/l2/8021x

802.1X Configuration Menu

```
[802.1x Configuration Menu]
     global   - Global 802.1x configuration menu
     port     - Port 802.1x configuration menu
     ena      - Enable 802.1x access control
     dis      - Disable 802.1x access control
     cur      - Show 802.1x configuration
```

This feature allows you to configure the CN4093 as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 207. 802.1X Configuration Menu (/cfg/l2/8021x)

Command Syntax and Usage
`global` Displays the global 802.1X Configuration Menu. To view menu options, see page 269.
`port` *<port alias or number>* Displays the 802.1X Port Menu. To view menu options, see page 272.
`ena` Globally enables 802.1X.
`dis` Globally disables 802.1X.
`cur` Displays current 802.1X parameters.

/cfg/l2/8021x/global

802.1X Global Configuration Menu

```
[802.1X Global Configuration Menu]
     gvlan    - 802.1X Guest VLAN configuration menu
     mode     - Set access control mode
     qtperiod - Set EAP-Request/Identity quiet time interval
     txperiod - Set EAP-Request/Identity retransmission timeout
     suptmout - Set EAP-Request retransmission timeout
     svrtmout - Set server authentication request timeout
     maxreq   - Set max number of EAP-Request retransmissions
     raperiod - Set reauthentication time interval
     reauth   - Set reauthentication status to on or off
     vassign  - Set dynamic VLAN assignment status to on or off
     default  - Restore default 802.1X configuration
     cur      - Display current 802.1X configuration
```

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

Table 208. 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)

Command Syntax and Usage
`gvlan` Displays the 802.1X Guest VLAN Configuration Menu. To view menu options, see page 271.
`mode force-unauth|auto|force-auth` Sets the type of access control for all ports: – `force-unauth`: the port is unauthorized unconditionally. – `auto`: the port is unauthorized until it is successfully authorized by the RADIUS server. – `force-auth`: the port is authorized unconditionally, allowing all traffic. The default value is `force-auth`.
`qtperiod` *<0-65535>* Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
`txperiod` *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
`suptmout` *<1-65535>* Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

Table 208. 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global) (continued)

Command Syntax and Usage
`svrtmout <1-65535>` Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `/cfg/sys/radius/timeout` (default is 3 seconds).
`maxreq <1-10>` Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
`raperiod <1-604800>` Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
`reauth on|off` Sets the re-authentication status to `on` or `off`. The default value is `off`.
`vassign on|off` Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`.
`default` Resets the global 802.1X parameters to their default values.
`cur` Displays current global 802.1X parameters.

/cfg/l2/8021x/global/gvlan

802.1X Guest VLAN Configuration Menu

```
[802.1X Guest VLAN Configuration Menu]
     vlan     - Set 8021.x Guest VLAN number
     ena      - Enable 8021.xGuest VLAN
     dis      - Disable 8021.x Guest VLAN
     cur      - Display current Guest VLAN configuration
```

The 802.1X Guest VLAN menu allows you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 209. 802.1X Guest VLAN Configuration Menu (/cfg/l2/8021x/global/gvlan)

Command Syntax and Usage
`vlan` *<VLAN number>* Configures the Guest VLAN number.
`ena` Enables the 802.1X Guest VLAN.
`dis` Disables the 802.1X Guest VLAN.
`cur` Displays current 802.1X Guest VLAN parameters.

/cfg/l2/8021x/port <*port alias or number*>

802.1X Port Configuration Menu

```
[802.1X Port Configuration Menu]
    mode     - Set access control mode
    qtperiod - Set EAP-Request/Identity quiet time interval
    txperiod - Set EAP-Request/Identity retransmission timeout
    suptmout - Set EAP-Request retransmission timeout
    svrtmout - Set server authentication request timeout
    maxreq   - Set max number of EAP-Request retransmissions
    raperiod - Set reauthentication time interval
    reauth   - Set reauthentication status to on or off
    vassign  - Set dynamic VLAN assignment status to on or off
    default  - Restore default 802.1X configuration
    global   - Apply current global 802.1X configuration to this port
    cur      - Display current 802.1X configuration
```

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

Table 210. 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

Command Syntax and Usage
`mode force-unauth|auto|force-auth` Sets the type of access control for the port: – `force-unauth` - the port is unauthorized unconditionally. – `auto` - the port is unauthorized until it is successfully authorized by the RADIUS server. – `force-auth` - the port is authorized unconditionally, allowing all traffic. The default value is `force-auth`.
`qtperiod` <*0-65535*> Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
`txperiod` <*1-65535*> Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
`suptmout` <*1-65535*> Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

Table 210. 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port) (continued)

Command Syntax and Usage
`svrtmout` *<1-65535>* Sets the time, in seconds, the authenticator waits for a response from the RADIUS server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `/cfg/sys/radius/timeout` (default is 3 seconds).
`maxreq` *<1-10>* Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
`raperiod` *<1-604800>* Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.
`reauth on|off` Sets the re-authentication status to `on` or `off`. The default value is `off`.
`vassign on|off` Sets the dynamic VLAN assignment status to `on` or `off`. The default value is `off`.
`default` Resets the 802.1X port parameters to their default values.
`global` Applies current global 802.1X configuration parameters to the port.
`cur` Displays current 802.1X port parameters.

/cfg/l2/mrst

RSTP/MSTP/PVRST Configuration Menu

```
[Multiple Spanning Tree Menu]
   cist     - Common and Internal Spanning Tree menu
   name     - Set MST region name
   rev      - Set revision level of this MST region
   maxhop   - Set Maximum Hop Count for MST (4 - 60)
   mode     - Spanning Tree Mode
   cur      - Display current MST parameters
```

IBM Networking OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), and Per VLAN Rapid Spanning Tree Protocol (PVRST). MSTP allows you to map many VLANs to a small number of Spanning Tree Groups (STGs), each with its own topology.

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

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

Table 211. MSTP/RSTP/PVRST Configuration Menu Options (/cfg/l2/mrst)

Command Syntax and Usage
`cist` Displays the Common Internal Spanning Tree (CIST) Menu. To view menu options, see page 275.
`name` *<1-32 characters>* Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.
`rev` *<0-65535>* Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within a MSTP region must have the same version number.
`maxhop` *<4-60>* Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default is 20.
`mode rstp|mstp|pvrst` Selects the Spanning Tree mode, as follows: Multiple Spanning Tree (`mstp`), Rapid Spanning Tree (`rstp`), Per VLAN Rapid Spanning Tree Plus (`pvrst`). The default mode is `STP/PVRST+`.
`cur` Displays the current RSTP/MSTP/PVRST+ configuration.

/cfg/l2/mrst/cist

Common Internal Spanning Tree Configuration Menu

```
[Common Internal Spanning Tree Menu]
  brg     - CIST Bridge parameter menu
  port    - CIST Port parameter menu
  add     - Add VLAN(s) to CIST
  default - Default Common Internal Spanning Tree and Member parameters
  cur     - Display current CIST parameters
```

Table 212 describes the commands used to configure Common Internal Spanning Tree (CIST) parameters. The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

Table 212. CIST Menu Options (/cfg/l2/mrst/cist)

Command Syntax and Usage
`brg` Displays the CIST Bridge Menu. To view menu options, see page 276.
`port` *<port alias or number>* Displays the CIST Port Menu. To view menu options, see page 277.
`add` *<VLAN numbers>* Adds selected VLANs to the CIST.
`default` Resets all CIST parameters to their default values.
`cur` Displays the current CIST configuration.

/cfg/l2/mrst/cist/brg

CIST Bridge Configuration Menu

```
[CIST Bridge Menu]
      prior   - Set CIST bridge Priority (0-65535)
      mxage   - Set CIST bridge Max Age (6-40 secs)
      fwd     - Set CIST bridge Forward Delay (4-30 secs)
      cur     - Display current CIST bridge parameters
```

CIST bridge parameters are used only when the switch is in MSTP mode. CIST parameters do not affect operation of STP/PVST+.

Table 213. CIST Bridge Configuration Menu Options (/cfg/l2/mrst/cist/brg)

Command Syntax and Usage
`prior` *<0-65535>* Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, in steps of 4096 (0, 4096, 8192...). The default value is 61440.
`mxage` *<6-40 seconds>* Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds.
`fwd` *<4-30 seconds>* Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.
`cur` Displays the current CIST bridge configuration.

/cfg/l2/mrst/cist/port <*port alias or number*>

CIST Port Configuration Menu

```
[CIST Port 1 Menu]
   prior    - Set port Priority (0-240)
   cost     - Set port Path Cost (1-200000000, 0 for auto)
   hello    - Set CIST port Hello Time (1-10 secs)
   pvst-pro - Enable/disable PVST Protection (for MSTP only)
   on       - Turn port's Spanning Tree ON
   off      - Turn port's Spanning Tree OFF
   cur      - Display current port Spanning Tree parameters
```

CIST port parameters are used to modify MRST operation on an individual port basis. CIST parameters do not affect operation of STP/PVST+, RSTP, or PVRST+. For each port, RSTP/MSTP is turned on by default.

Table 214. CIST Port Configuration Menu Options (/cfg/l2/mrst/cist/port)

Command Syntax and Usage
`prior` *<0-240>* Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.
`cost` *<0-200000000>* Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: – 100Mbps = 200000 – 1Gbps = 20000 – 10Gbps = 2000 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.
`hello` *<1-10 seconds>* Configures the CIST port Hello time.The Hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge Hello value. The range is 1 to 10 seconds, and the default is 2 seconds.
`pvst-pro enable|disable` Enables or disables PVST Protection on the selected port. If the port receives any PVST+/PVRST+ BPDUs, it error disabled. PVST Protection works only in MSTP mode. The default setting is `disabled`.
`on` Enables MRST on the port.

Table 214. CIST Port Configuration Menu Options (/cfg/l2/mrst/cist/port) (continued)

Command Syntax and Usage
`off` Disables MRST on the port.
`cur` Displays the current CIST port configuration.

/cfg/l2/stg <*STP group index*>
Spanning Tree Configuration Menu

```
[Spanning Tree Group 1 Menu]
      brg     - Bridge parameter menu
      port    - Port parameter menu
      add     - Add VLAN(s) to Spanning Tree Group
      remove  - Remove VLAN(s) from Spanning Tree Group
      clear   - Remove all VLANs from Spanning Tree Group
      on      - Globally turn Spanning Tree ON
      off     - Globally turn Spanning Tree OFF
      default - Default Spanning Tree and Member parameters
      cur     - Display current bridge parameters
```

IBM Networking OS supports the IEEE 802.1D Spanning Tree Protocol (STP). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG reserved for management).

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

Table 215. Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage
`brg` Displays the Bridge Spanning Tree Menu. To view menu options, see page 279.
`port` <*port alias or number*> Displays the Spanning Tree Port Menu. To view menu options, see page 280.
`add` <*VLAN number*> Associates a VLAN with a Spanning Tree and requires a VLAN ID as a parameter.
`remove` <*VLAN number*> Breaks the association between a VLAN and a Spanning Tree and requires a VLAN ID as a parameter.
`clear` Removes all VLANs from a Spanning Tree.
`on` Globally enables Spanning Tree Protocol. STG is turned on by default.

Table 215. Spanning Tree Configuration Menu (/cfg/l2/stg) (continued)

Command Syntax and Usage
`off` Globally disables Spanning Tree Protocol.
`default` Restores a Spanning Tree instance to its default configuration.
`cur` Displays current Spanning Tree Protocol parameters.

/cfg/l2/stg <*STP group number*>/brg
Spanning Tree Bridge Configuration Menu

```
[Bridge Spanning Tree Menu]
      prior   - Set bridge Priority [0-65535]
      hello   - Set bridge Hello Time [1-10 secs]
      mxage   - Set bridge Max Age (6-40 secs)
      fwd     - Set bridge Forward Delay (4-30 secs)
      cur     - Display current bridge parameters
```

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

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

Table 216. Spanning Tree Bridge Menu Options (/cfg/l2/stg/brg)

Command Syntax and Usage
`prior` <*new bridge priority (0-65535)*> Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The default value is 65534. **RSTP/MSTP**: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 61440.
`hello` <*new bridge hello time (1-10 secs)*> Configures the bridge hello time.The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds. This command does not apply to MSTP (see CIST on page 275).

Table 216. Spanning Tree Bridge Menu Options (/cfg/l2/stg/brg) (continued)

Command Syntax and Usage
`mxage` *<new bridge max age (6-40 secs)>* Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STG network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to MSTP (see CIST on page 275).
`fwd` *<new bridge Forward Delay (4-30 secs)>* Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to MSTP (see CIST on page 275).
`cur` Displays the current bridge STG parameters.

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

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

/cfg/l2/stg *<STP group index>*/port *<port alias or number>*

Spanning Tree Port Configuration Menu

```
[Spanning Tree Port EXT1 Menu]
  prior    - Set port Priority (0-255)
  cost     - Set port Path Cost (1-65535 (802.1D) /
             1-200000000 (MSTP/RSTP) /0 for auto)
  on       - Turn port's Spanning Tree ON
  off      - Turn port's Spanning Tree OFF
  cur      - Display current port Spanning Tree parameters
```

By default for STP/PVST+, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports. By default for RSTP/MSTP, Spanning Tree is turned off for internal ports and management ports, and turned on for external ports, with internal ports configured as edge ports. STG port parameters include:

- Port priority
- Port path cost

For more information about port Spanning Tree commands, see "Port Spanning Tree Configuration Menu" on page 239.

Table 217. Spanning Tree Port Menu Options (/cfg/l2/stg/port)

Command Syntax and Usage
`prior` *<new port Priority (0-255)>* Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...).
`cost` *<1-65535, 0 for default)>* Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Port path cost is based on the port speed, and is calculated as follows: – 100Mbps = 19 – 1Gbps = 4 – 10Gbps = 2 The default value of 0 (zero) indicates that the default path cost will be computed for an auto negotiated link speed.
`on` Enables STG on the port.
`off` Disables STG on the port.
`cur` Displays the current STG port parameters.

/cfg/l2/fdb
Forwarding Database Configuration Menu

```
[FDB Menu]
     mcast    - Static Multicast Menu
     static   - Static FDB Menu
     aging    - Configure FDB aging value
     cur      - Display current FDB configuration
```

Use the following commands to configure the Forwarding Database (FDB) for the CN4093.

Table 218. FDB Menu Options (/cfg/l2/fdb)

Command Syntax and Usage
`mcast` Displays the static Multicast menu. To view menu options, see page 282.
`static` Displays the static FDB menu. To view menu options, see page 283.
`aging` *<0-65535>* Configures the aging value for FDB entries, in seconds. The default value is 300.
`cur` Displays the current FDB parameters.

/cfg/l2/fdb/mcast
Static Multicast MAC Configuration Menu

```
[Static Multicast Menu]
     add      - Add a Multicast Address entry
     del      - Delete a Multicast Address entry
     clear    - Clear all Multicast Address entries
     cur      - Display current Multicast Address 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 (`/cfg/l2/fdb/mcast/add`).
- 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 (`/cfg/l2/fdb/mcast/add`).
  - Enable Flood Blocking on ports that are not to receive multicast packets (`/cfg/port` *x*`/floodblk ena`).

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

Table 219. Static Multicast MAC Menu Options (/cfg/l2/fdb/mcast)

Command Syntax and Usage
`add` *<MAC address> <VLAN number>* {`port` *<port alias or number>*| `trunk` *<trunk number>*|`adminkey` *<1-65535>*} 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: `add 01:00:00:23:3f:01 200 int1-int4`
`del` *<MAC address> <VLAN number> <port alias or number>* Deletes a static multicast entry.
`clear` {`all`|`mac` *<MAC address>*|`vlan` *<VLAN number>*| `port` *<port alias or number>*|`trunk` *<trunk number>*|`adminkey` *<1-65535>*} Clears static multicast entries.
`cur` Display current static multicast entries.

/cfg/l2/fdb/static
Static FDB Configuration Menu

```
[Static FDB Menu]
     add      - Add a permanent FDB entry
     del      - Delete a static FDB entry
     clear    - Clear static FDB entries
     cur      - Display current static FDB configuration
```

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

Table 220. Static FDB Menu Options (/cfg/l2/fdb/static)

Command Syntax and Usage
`add` *<MAC address> <VLAN number>* {`port` *<port alias or number>*| `trunk` *<trunk number>*|`adminkey` *<value>*} 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`
`del` *<MAC address> <VLAN number>* Deletes a permanent FDB entry.

Table 220. Static FDB Menu Options (/cfg/l2/fdb/static) (continued)

Command Syntax and Usage
`clear` *<MAC address>*`|all {mac|vlan|port}` Clears static FDB entries.
`cur` Display current static FDB configuration.

/cfg/l2/ecp
ECP Configuration

```
[Edge Control Protocol Configuration Menu]
     retrans  - Set ECP retransmission interval
     cur      - Show current ECP parameters
```

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

Table 221. ECP Configuration Options

Command Syntax and Usage
`retrans` *<retransmission value>* Sets the retransmission value, in milliseconds. The default value is 1000ms.
`cur` Display the current ECP configuration.

/cfg/l2/lldp

LLDP Configuration Menu

```
[LLDP configuration Menu]
     port     - LLDP Port Menu
     msgtxint - Set transmission interval for LLDPDU
     msgtxhld - Set holdtime multiplier for LLDP advertisement
     notifint - Set minimum interval for successive trap notification
     txdelay  - Set delay interval between LLDP advertisements
     redelay  - Set reinitialization delay interval
     on       - Globally turn LLDP On
     off      - Globally turn LLDP Off
     cur      - Show current LLDP parameters
```

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

Table 222. LLDP Menu Options (/cfg/l2/lldp)

Command Syntax and Usage
`port` *<port alias or number>* Displays the LLDP Port Configuration menu. To view menu options, see page 286.
`msgtxint` *<5-32768>* Configures the message transmission interval, in seconds. The default value is 30.
`msgtxhld` *<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.
`notifint` *<1-3600>* Configures the trap notification interval, in seconds. The default value is 5.
`txdelay` *<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.
`redelay` *<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.
`on` Globally turns LLDP on. The default setting is `on`.

Table 222. LLDP Menu Options (/cfg/l2/lldp) (continued)

Command Syntax and Usage
`off` Globally turns LLDP off.
`cur` Display current LLDP configuration.

/cfg/l2/lldp/port <*port alias or number*>

LLDP Port Configuration Menu

```
[LLDP Port EXT2 Menu]
     admstat  - Set LLDP admin-status of this port
     snmptrap - Enable/disable SNMP trap notification of this port
     tlv      - Optional TLVs Menu
     cur      - Show current LLDP port parameters
```

Use the following commands to configure LLDP port options.

Table 223. LLDP Port Menu Options (/cfg/l2/lldp/port)

Command Syntax and Usage
`admstat 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 value is `tx_rx`.
`snmptrap e|d` Enables or disables SNMP trap notification for LLDP messages.
`tlv` Displays the Optional TLV menu for the selected port. To view menu options, see page 287.
`cur` Display current LLDP configuration.

/cfg/l2/lldp/port <*port alias or number*>/tlv
LLDP Optional TLV Configuration Menu

```
[Optional TLVs Menu]
portdesc - Enable/disable Port Description TLV for this port
sysname  - Enable/disable System Name TLV for this port
sysdescr - Enable/disable System Description TLV for this port
syscap   - Enable/disable System Capabilities TLV for this port
mgmtaddr - Enable/disable Management Address TLV for this port
portvid  - Enable/disable Port VLAN ID TLV for this port
portprot - Enable/disable Port and Protocol VLAN ID TLV for this port
vlanname - Enable/disable VLAN Name TLV for this port
protid   - Enable/disable Protocol Identity TLV for this port
macphy   - Enable/disable MAC/PHY Configuration/Status TLV for this port
powermdi - Enable/disable Power Via MDI TLV for this port
linkaggr - Enable/disable Link Aggregation TLV for this port
framesz  - Enable/disable Maximum Frame Size TLV for this port
dcbx     - Enable/disable DCBX TLV for this port
all      - Enable/disable all the Optional TLVs for this port
cur      - Display current Optional TLVs configuration
```

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

Table 224. Optional TLV Menu Options (/cfg/l2/lldp/port x/tlv)

Command Syntax and Usage
`portdesc d|e` Enables or disables the Port Description information type.
`sysname d|e` Enables or disables the System Name information type.
`sysdescr d|e` Enables or disables the System Description information type.
`syscap d|e` Enables or disables the System Capabilities information type.
`mgmtaddr d|e` Enables or disables the Management Address information type.
`portvid d|e` Enables or disables the Port VLAN ID information type.
`portprot d|e` Enables or disables the Port and VLAN Protocol ID information type.
`vlanname d|e` Enables or disables the VLAN Name information type.
`protid d|e` Enables or disables the Protocol ID information type.

Table 224. Optional TLV Menu Options (/cfg/l2/lldp/port x/tlv) (continued)

Command Syntax and Usage
`macphy d|e` Enables or disables the MAC/Phy Configuration information type.
`powermdi d|e` Enables or disables the Power via MDI information type.
`linkaggr d|e` Enables or disables the Link Aggregation information type.
`framesz d|e` Enables or disables the Maximum Frame Size information type.
`dcbx d|e` Enables or disables the Data Center Bridging Capability Exchange (DCBX) information type.
`all d|e` Enables or disables all optional TLV information types.
`cur` Display current Optional TLV configuration.

/cfg/l2/trunk <*trunk group number*>
Trunk Configuration Menu

```
[Trunk group 1 Menu]
      add     - Add port to trunk group
      rem     - Remove port from trunk group
      ena     - Enable trunk group
      dis     - Disable trunk group
      del     - Delete trunk group
      cur     - Display current Trunk Group configuration
```

Trunk groups can provide super-bandwidth connections between CN4093s 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 CN4093, with the following restrictions:

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

By default, each trunk group is empty and disabled.

Table 225. Trunk Configuration Menu Options (/cfg/l2/trunk)

Command Syntax and Usage
`add` *<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 (-).
`rem` *<port alias or number>* Removes a physical port or ports from the current trunk group.
`ena` Enables the current trunk group.
`dis` Disables the current trunk group.
`del` Removes the current trunk group configuration.
`cur` Displays current trunk group parameters.

/cfg/l2/thash
Trunk Hash Configuration Menu

```
[Trunk Hash Menu]
     l2thash  - L2 Trunk Hash Control
     l3thash  - L3 Trunk Hash Control
     ingress  - Enable/disable ingress port hash
     L4port   - Enable/disable L4 port hash
     cur      - Display current Trunk Hash configuration
```

Use the following commands to configure IP trunk hash settings for the CN4093. Trunk hash parameters are set globally for the CN4093. The trunk hash settings affect both static trunks and LACP trunks.

To achieve the most even traffic distribution, select options that exhibit a wide range of values for your particular network. You may use the configuration settings listed in Table 226 combined with the hash parameters listed in Table 227.

Table 226. Trunk Hash Settings (/cfg/l2/thash)

Command Syntax and Usage
`l2thash` Displays the Layer 2 Trunk Hash Settings menu. To view menu options, see page 290.
`l3thash` Displays the Layer 3 Trunk Hash Settings menu. To view menu options, see page 291.

Table 226. Trunk Hash Settings (/cfg/l2/thash) (continued)

Command Syntax and Usage
`ingress e|d` Enables or disables trunk hash computation based on the ingress port. The default setting is `disabled`.
`L4port e|d` Enables or disables use of Layer 4 service ports (TCP, UDP, and so on) to compute the hash value. The default setting is `disabled`.
`cur` Display current trunk hash configuration.

/cfg/l2/thash/l2thash

Layer 2 Trunk Hash Menu

```
[L2 Trunk Hash Menu]
     smac     - Enable/disable smac hash
     dmac     - Enable/disable dmac hash
     cur      - Display current trunk hash setting for L2 traffic
```

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 227. Layer 2 Trunk Hash Options (/cfg/l2/thash/l2thash)

Command Syntax and Usage
`smac enable|disable` Enables or disable Layer 2 trunk hashing on the source MAC.
`dmac enable|disable` Enables or disable Layer 2 trunk hashing on the destination MAC.
`cur` Displays current Layer 2 trunk hash settings.

/cfg/l2/thash/l3thash

Layer 3 Trunk Hash Menu

```
[L3 Trunk Hash Menu]
     useL2    - Enable/disable L2 hash for IP packet
     sip      - Enable/disable sip hash for IP packet
     dip      - Enable/disable dip hash for IP packet
     cur      - Display current trunk hash setting for L3 traffic
```

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 228. Layer 3 Trunk Hash Options (/cfg/l2/thash/l3thash)

Command Syntax and Usage
`useL2 enable|disable` Enables or disables use of Layer 2 hash parameters only. When enabled, Layer 3 hashing parameters are cleared.
`sip enable|disable` Enables or disables Layer 3 trunk hashing on the source IP address.
`dip enable|disable` Enables or disables Layer 3 trunk hashing on the destination IP address.
`cur` Displays current Layer 3 trunk hash settings.

/cfg/l2/vlag

Virtual Link Aggregation Control Protocol Configuration

```
[vLAG Menu]
     trunk    - Set vLAG underlying Trunk
     adminkey - Set vLAG underlying LACP channel
     hlthchk  - Set vLAG Health Check Menu
     isl      - Set ISL properties
     enable   - Enable vLAG globally
     disable  - Disable vLAG globally
     tier-id  - Set vLAG Tier ID
     priority - Set vLAG priority
     delay    - Set vLAG Startup Delay interval
     cur      - Display current vLAG configuration
```

vLAG groups allow you to enhance redundancy and prevent implicit loops without using STP. The vLAG group acts as a single virtual entity for the purpose of establishing a multi-port trunk.

Table 229. vLAG Configuration Options

Command Syntax and Usage
`trunk` *<trunk group number>* Defines a trunk group as a vLAG. To view menu options, see page 293.
`adminkey` *<1-65535>* Defines an LACP *admin key* as a vLAG. LACP trunks formed with this *admin key* will be included in the vLAG configuration. To view menu options, see page 293.
`hlthchk` Displays the vLAG health check menu. To view menu options, see page 293.
`isl` Displays the ISL Configuration menu. To view menu options, see page 294.
`enable` Enables vLAG globally.
`disable` Disables vLAG globally.
`tier-id` *<0-512>* Sets the vLAG peer ID. To disable this, set the vLAG peer ID to 0 (zero).
`priority` *<0-65535>* Configures the vLAG priority for the switch, used for election of Primary and Secondary vLAG switches. The switch with lower priority is elected to the role of Primary vLAG switch.
`delay` *<0-3600 seconds>* Sets the vLAG startup delay interval, in seconds.
`cur` Displays current vLAG parameters.

/cfg/l2/vlag/trunk <*trunk ID*>

vLAG Trunk Configuration

```
[vLAG trunk 4 Menu]
     ena      - Enable a vLAG
     dis      - Disable a vLAG
     cur      - Display current vLAG configuration
```

Table 230. vLAG Trunk Configuration Options

Command Syntax and Usage
ena Enables vLAG on the selected trunk group.
dis Disables vLAG on the selected trunk group.
cur Displays current vLAG trunk parameters.

/cfg/l2/vlag/adminkey <*1-65535*>

vLAG LACP Configuration

```
[Set vLAG underlying LACP channel]
     ena      - Enable a vLAG
     dis      - Disable a vLAG
     cur      - Display current vLAG configuration
```

Table 231. vLAG LACP Configuration Options

Command Syntax and Usage
ena Enables vLAG on LACP trunks formed from the selected LACP *admin key*.
dis Disables vLAG on LACP trunks formed from the selected LACP *admin key*.
cur Displays current vLAG LACP parameters.

/cfg/l2/vlag/hlthchk

vLAG Health Check Configuration

```
[vLAG Health Check Menu]
     peer-ip               - Set health check peer ip
     connect-retry-interval - Set health check Connect-retry interval
     keepalive-attempts     - Set health check keepalive attempts
     keepalive-interval     - Set health check Keepalive interval
```

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

Table 232. vLAG Health Check Configuration Options

Command Syntax and Usage
`peer-ip` *<IP address>* Configures the IP address of the vLAG peer.
`connect-retry-interval` *<1-300>* Sets the vLAG health check connect retry interval, in seconds. The default value is 30.
`keepalive-attempts` *<1-24>* Sets the number of vLAG keep alive attempts. The default value is 3.
`keepalive-interval` *<2-300>* Sets the time between vLAG keep alive attempts, in seconds. The default value is 5.

/cfg/l2/vlag/isl

vLAG ISL Configuration

```
[vLAG ISL Menu]
     trunk    - Set ISL Trunk
     adminkey - Set ISL LACP channel
     vlan     - Set ISL VLAN
     cur      - Display current vLAG configuration
```

These commands allow you to configure a dedicated inter-switch link (ISL) for synchronization between vLAG peers.

Table 233. vLAG ISL Configuration Options

Command Syntax and Usage
`trunk` *<trunk group number>* Defines a trunk group used for the vLAG Inter-Switch Link (ISL).
`adminkey` *<1-65535>* Defines an LACP *admin key* used for the vLAG Inter-Switch Link (ISL). LACP trunks formed with this *admin key* will be included in the ISL.

Table 233. vLAG ISL Configuration Options

Command Syntax and Usage
`vlan` *<VLAN number>* Defines the VLAN used to carry vLAG protocol data.
`cur` Displays current vLAG ISL parameters.

/cfg/l2/lacp
LACP Configuration Menu

```
[LACP Menu]
     port     - LACP Port Menu
     sysprio  - Set LACP system priority
     timeout  - Set LACP system timeout scale for timing out partner
                info
     delete   - Delete an LACP trunk
     default  - Restore default LACP system configuration
     cur      - Display current LACP configuration
```

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

Table 234. LACP Menu Options (/cfg/l2/lacp)

Command Syntax and Usage
`port` *<port alias or number>* Displays the LACP Port menu. To view menu options, see page 296.
`sysprio` *<1-65535>* Defines the priority value (1 through 65535) for the CN4093. Lower numbers provide higher priority. The default value is 32768.
`timeout short|long` Defines the timeout period before invalidating LACP data from a remote partner. Choose `short` (3 seconds) or `long` (90 seconds). The default value is `long`. **Note**: It is recommended that you use a timeout value of `long`, to reduce LACPDU processing. If your CN4093's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.
`delete` *<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*.

Table 234. LACP Menu Options (/cfg/l2/lacp) (continued)

Command Syntax and Usage
`default sysprio|timeout` Restores the selected parameters to their default values.
`cur` Display current LACP configuration.

/cfg/l2/lacp/port <*port alias or number*>
LACP Port Configuration Menu

```
[LACP Port EXT1 Menu]
     mode     - Set LACP mode
     prio     - Set LACP port priority
     adminkey - Set LACP port admin key
     minlinks - Set LACP port minimum links
     default  - Restore default LACP port configuration
     cur      - Display current LACP port configuration
```

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

Table 235. LACP Port Menu Options (/cfg/l2/lacp/port)

Command Syntax and Usage
`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.
`prio` <*1-65535*> Sets the priority value for the selected port. Lower numbers provide higher priority. The default value is 32768.
`adminkey` <*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.
`minlinks` <*1-16*> Set the minimum number of links for this port. If the specified minimum number of ports are not available, the trunk is placed in the `down` state.

Table 235. LACP Port Menu Options (/cfg/l2/lacp/port) (continued)

Command Syntax and Usage
`default adminkey|mode|prio` Restores the selected parameters to their default values.
`cur` Displays the current LACP configuration for this port.

/cfg/l2/failovr
Layer 2 Failover Configuration Menu

```
[Failover Menu]
     trigger  - Trigger Menu
     vlan     - Globally turn VLAN Monitor ON/OFF
     on       - Globally turn Failover ON
     off      - Globally turn Failover OFF
     cur      - Display current Failover configuration
```

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

Table 236. Layer 2 Failover Menu Options (/cfg/l2/failovr)

Command Syntax and Usage
`trigger <1-8>` Displays the Failover Trigger menu. To view menu options, see page 298.
`vlan on|off` Globally turns VLAN monitor `on` or `off`. When the VLAN Monitor is `on`, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is `off`.
`on` Globally turns Layer 2 Failover `on`.
`off` Globally turns Layer 2 Failover `off`.
`cur` Displays current Layer 2 Failover parameters.

/cfg/l2/failovr/trigger <1-8>

Failover Trigger Configuration Menu

```
[Trigger 1 Menu]
     amon     - Auto Monitor Menu
     mmon     - Manual Monitor Menu
     limit    - Limit of Trigger
     ena      - Enable Trigger
     dis      - Disable Trigger
     del      - Delete Trigger
     cur      - Display current Trigger configuration
```

Table 237. Failover Trigger Menu Options (/cfg/l2/failovr/trigger)

Command Syntax and Usage
amon Displays the Auto Monitor menu for the selected trigger. To view menu options, see page 299.
mmon Displays the Manual Monitor menu for the selected trigger. To view menu options, see page 299.
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.
ena Enables the selected trigger.
dis Disables the selected trigger.
del Deletes the selected trigger.
cur Displays the current failover trigger settings.

/cfg/l2/failovr/trigger <1-8>/amon

Auto Monitor Configuration Menu

```
[Auto Monitor Menu]
     addtrnk  - Add trunk to Auto Monitor
     remtrnk  - Remove trunk from Auto Monitor
     addkey   - Add LACP port adminkey to Auto Monitor
     remkey   - Remove LACP port adminkey from Auto Monitor
     cur      - Display current Auto Monitor configuration
```

Table 238. Auto Monitor Menu Options (/cfg/l2/failovr/trigger/amon)

Command Syntax and Usage
addtrnk <*trunk group number)*> Adds a trunk group to the Auto Monitor.
remtrnk <*trunk group number*> Removes a trunk group from the Auto Monitor.
addkey <*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.
remkey <*1-65535*> Removes an LACP *admin key* from the Auto Monitor.
cur Displays the current Auto Monitor settings.

/cfg/l2/failovr/trigger <1-8>/mmon

Manual Monitor Configuration Menu

```
[Manual Monitor Menu]
     monitor  - Monitor Menu
     control  - Control Menu
     cur      - Display current Manual Monitor configuration
```

Use this menu to configure Failover Manual Monitor. These menus allow you to manually define both the monitor and control ports that participate in failover teaming.

Note: AMON and MMON configurations are mutually exclusive.

Table 239. Failover Manual Monitor options (/cfg/l2/failovr/trigger/mmon)

Command Syntax and Usage
monitor Displays the Manual Monitor - Monitor menu for the selected trigger.

Table 239. Failover Manual Monitor options (/cfg/l2/failovr/trigger/mmon) (continued)

Command Syntax and Usage
control Displays the Manual Monitor - Control menu for the selected trigger.
cur Displays the current Manual Monitor settings.

/cfg/l2/failovr/trigger <1-8>/mmon/monitor

Manual Monitor Port Configuration Menu

```
[Monitor Menu]
     addport  - Add port to Monitor
     remport  - Remove port from Monitor
     addtrnk  - Add trunk to Monitor
     remtrnk  - Remove trunk from Monitor
     addkey   - Add LACP port adminkey to Monitor
     remkey   - Remove LACP port adminkey from Monitor
     cur      - Display current Monitor configuration
```

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

Table 240. Failover Manual Monitor Port Options (/cfg/l2/failovr/trigger/mmon/monitor)

Command Syntax and Usage
addport <*port alias or number*> Adds the selected port to the Manual Monitor Port configuration.
remport <*port alias or number*> Removes the selected port from the Manual Monitor Port configuration.
addtrnk <*trunk number*> Adds a trunk group to the Manual Monitor Port configuration.
remtrnk <*trunk number*> Removes a trunk group from the Manual Monitor Port configuration.
addkey <*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.
remkey <*1-65535*> Removes an LACP admin key from the Manual Monitor Port configuration.
cur Displays the current Manual Monitor Port configuration.

/cfg/l2/failovr/trigger <*1-8*>/mmon/control

Manual Monitor Control Configuration Menu

```
[Control Menu]
     addport  - Add port to Control
     remport  - Remove port from Control
     addtrnk  - Add trunk to Control
     remtrnk  - Remove trunk from Control
     addkey   - Add LACP port adminkey to Control
     remkey   - Remove LACP port adminkey from Control
     cur      - Display current Control configuration
```

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

Table 241. Failover Manual Monitor Control Options (/cfg/l2/failovr/trigger/mmon/control)

Command Syntax and Usage
addport <*port alias or number*> Adds the selected port to the Manual Monitor Control configuration.
remport <*port alias or number*> Removes the selected port from the Manual Monitor Control configuration.
addtrnk <*trunk number*> Adds a trunk group to the Manual Monitor Control configuration.
remtrnk <*trunk number*> Removes a trunk group from the Manual Monitor Control configuration.
addkey <*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.
remkey <*1-65535*> Removes an LACP *admin key* from the Manual Monitor Control configuration.
cur Displays the current Manual Monitor Control configuration.

/cfg/l2/hotlink
Hot Links Configuration Menu

```
[Hot Links Menu]
     trigger  - Trigger Menu
     bpdu     - Enable/disable BPDU flood
     sndfdb   - Enable/disable FDB update
     sndrate  - Set FDB update rate
     on       - Globally turn Hot Links ON
     off      - Globally turn Hot Links OFF
     cur      - Display current Hot Links configuration
```

Table 242 describes the Hot Links menu options.

Table 242. Hot Links Menu Options (/cfg/l2/hotlink)

Command Syntax and Usage
`trigger` *<1-25>* Displays the Hot Links Trigger menu. To view menu options, see page 303.
`bpdu enable|disable` Enables or disables flooding of Spanning-Tree BPDUs on the active Hot Links interface when the interface belongs to a Spanning Tree group that is globally turned `off`. This feature can prevent unintentional loop scenarios (for example, if two uplinks come up at the same time). The default setting is `disabled`.
`sndfdb enable|disable` Enables or disables FDB Update, which allows the switch to send FDB and MAC update packets over the active interface. The default setting is `disabled`.
`sndrate` *<10-1000>* Configures the FDB Update rate, in packets per second.
`on` Globally turns Hot Links `on`. The default value is `off`.
`off` Globally turns Hot Links `off`.
`cur` Displays current Hot Links configuration.

/cfg/l2/hotlink/trigger <1-25>

Hot Links Trigger Configuration Menu

```
[Trigger 2 Menu]
     master   - Master Menu
     backup   - Backup Menu
     fdelay   - Set Forward Delay (secs)
     name     - Set Trigger Name
     preempt  - Enable/disable Preemption
     ena      - Enable Trigger
     dis      - Disable Trigger
     del      - Delete Trigger
     cur      - Display current Trigger configuration
```

Table 243. Hot Links Trigger Menu Options (/cfg/l2/hotlink/trigger)

Command Syntax and Usage
`master` Displays the Master interface menu for the selected trigger. To view menu options, see page 304.
`backup` Displays the Backup interface menu for the selected trigger. To view menu options, see page 304.
`fdelay` *<0-3600>* Configures the Forward Delay interval, in seconds. The default value is `1`.
`name` *<1-32 characters>* Configures a name for the trigger.
`preempt e|d` Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default setting is `enabled`.
`ena` Enables the Hot Links trigger.
`dis` Disables the Hot Links trigger.
`del` Deletes the Hot Links trigger.
`cur` Displays the current Hot Links trigger configuration.

/cfg/l2/hotlink/trigger <*1-25*>/master

Hot Links Trigger Master Configuration Menu

```
[Master Menu]
     port     - Set port in Master
     trunk    - Set trunk in Master
     adminkey - Set adminkey in Master
     cur      - Display current Master configuration
```

Table 244. Hot Links Trigger Master menu (/cfg/l2/hotlink/trigger/master)

Command Syntax and Usage
port <*port alias or number*> Adds the selected port to the Master interface. Enter 0 (zero) to clear the port.
trunk <*trunk number*> | 0 Adds the selected trunk group to the Master interface. Enter 0 (zero) to clear the trunk group.
adminkey <*1-65535*> Adds an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* will be included in the Master interface. Enter 0 (zero) to clear the *admin key*.
cur Displays the current Hot Links Master interface configuration.

/cfg/l2/hotlink/trigger <*1-25*>/backup

Hot Links Trigger Backup Configuration Menu

```
[Backup Menu]
     port     - Set port in Backup
     trunk    - Set trunk in Backup
     adminkey - Set adminkey in Backup
     cur      - Display current Backup configuration
```

Table 245. Hot Links Trigger Backup menu (/cfg/l2/hotlink/trigger/backup)

Command Syntax and Usage
port <*port alias or number*> Adds the selected port to the Backup interface. Enter 0 (zero) to clear the port.
trunk <*trunk number*> | 0 Adds the selected trunk to the Backup interface. Enter 0 (zero) to clear the trunk group.

Table 245. Hot Links Trigger Backup menu (/cfg/l2/hotlink/trigger/backup) (continued)

Command Syntax and Usage
`adminkey <1-65535>` Adds an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* will be included in the Backup interface. Enter 0 (zero) to clear the *admin key*.
`cur` Displays the current Hot Links Backup interface settings.

/cfg/l2/vlan <*VLAN number*>
VLAN Configuration Menu

```
[VLAN 1 Menu]
     pvlan    - Protocol VLAN Menu
     privlan  - Private-VLAN Menu
     name     - Set VLAN name
     stg      - Assign VLAN to a Spanning Tree Group
     vmap     - Set VMAP for this vlan
     add      - Add port to VLAN
     rem      - Remove port from VLAN
     def      - Define VLAN as list of ports
     mgmt     - Enable/Disable this VLAN as additional management VLAN
     ena      - Enable VLAN
     dis      - Disable VLAN
     del      - Delete VLAN
     cur      - Display current VLAN configuration
```

The commands in this menu configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs.

By default, VLAN 1 is the only VLAN configured on the switch. Internal server ports and external uplink ports are members of VLAN 1 by default. Up to 4094 VLANs can be configured on the CN4093.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 246. VLAN Configuration Menu Options (/cfg/l2/vlan)

Command Syntax and Usage
`pvlan <1-8>` Displays the Protocol-based VLAN menu. To view menu options, see page 307.
`privlan` Displays the Private VLAN menu. To view menu options, see page 309.
`name` Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.

Table 246. VLAN Configuration Menu Options (/cfg/l2/vlan) (continued)

Command Syntax and Usage
`stg` *<Spanning Tree Group index>* Assigns a VLAN to a Spanning Tree Group.
`vmap {add|rem} <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.
`add` *<port alias or number>* Adds port(s) to the VLAN membership.
`rem` *<port alias or number>* Removes port(s) from this VLAN.
`def` *<list of port numbers>* Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, internal server ports (INT*x*) and external ports (EXT*x*) are in VLAN 1.
`mgmt enable|disable` Configures this VLAN as a management VLAN. You must add the management ports to each new management VLAN. External ports cannot be added to management VLANs.
`ena` Enables this VLAN.
`dis` Disables this VLAN without removing it from the configuration.
`del` Deletes this VLAN.
`cur` Displays the current VLAN configuration.

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 remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on (see the `tag` command on page 232).

/cfg/l2/vlan/pvlan <*protocol number*>
Protocol-Based VLAN Configuration Menu

```
[VLAN 1 Protocol 1 Menu]
     pty      - Set protocol type
     protocol - Select a predefined protocol
     prio     - Set priority to protocol
     add      - Add port to PVLAN
     rem      - Remove port from PVLAN
     ports    - Add/Remove a list of ports to/from PVLAN
     tagpvl   - Enable/Disable port tagging for PVLAN
     taglist  - Enable tagging a port list for PVLAN
     ena      - Enable protocol
     dis      - Disable protocol
     del      - Delete protocol
     cur      - Display current PVLAN configuration
```

Use this menu to configure Protocol-based VLAN (PVLAN) for the selected VLAN.

Table 247. PVLAN Menu Options (/cfg/l2/vlan/pvlan)

Command Syntax and Usage
`pty` *<(Ether2|SNAP|LLC)> <Ethernet type>* Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as `0080` (IPv4).
`protocol` *<Protocol type>* Selects a pre-defined protocol, as follows: – `decEther2`:DEC Local Area Transport – `ipv4Ether2`:Internet IP (IPv4) – `ipv6Ether2`:IPv6 – `ipx802.2`:Novell IPX 802.2 – `ipx802.3`:Novell IPX 802.3 – `ipxEther2`:Novell IPX – `ipxSnap`:Novell IPX SNAP – `netbios`:NetBIOS 802.2 – `rarpEther2`:Reverse ARP – `sna802.2`:SNA 802.2 – `snaEther2`:IBM SNA Service on Ethernet – `vinesEther2`:Banyan VINES – `xnsEther2`:XNS Compatibility
`prio` *<0-7>* Configures the priority value for this PVLAN.
`add` *<port alias or number>* Adds a port to the selected PVLAN.
`rem` *<port alias or number>* Removes a port from the selected PVLAN.

Table 247. PVLAN Menu Options (/cfg/l2/vlan/pvlan) (continued)

Command Syntax and Usage
`ports` *<port alias or number, or a list or range of ports>* Defines a list of ports that belong to the selected protocol on this VLAN. Enter 0 (zero) to remove all ports.
`tagpvl enable|disable` Enables or disables port tagging on this PVLAN.
`taglist` {*<port alias or number, or a list or range of ports>*|`empty`} Defines a list of ports that will be tagged by the selected protocol on this VLAN. Enter `empty` to disable tagging on all ports by this PVLAN.
`ena` Enables the selected protocol on the VLAN.
`dis` Disables the selected protocol on the VLAN.
`del` Deletes the selected protocol configuration from the VLAN.
`cur` Displays current parameters for the selected PVLAN.

/cfg/l2/vlan/privlan
Private VLAN Configuration Menu

```
[privlan Menu]
     type     - Set Private-VLAN type
     map      - Associate secondary VLAN with a primary VLAN
     ena      - Enable Private-VLAN
     dis      - Disable Private-VLAN
     cur      - Display current Private-VLAN configuration
```

Use this menu to configure a Private VLAN.

Table 248. Private VLAN Menu Options (/cfg/l2/vlan/privlan)

Command Syntax and Usage
type {none|primary|isolated|community} Defines the VLAN type, as follows: – none: Clears the Private VLAN type. – primary: 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. – isolated: The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN. – community: Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.
map <*2-4094*>|none Configures Private VLAN mapping between a secondary VLAN (isolated or community) and a primary VLAN. Enter the primary VLAN ID.
ena Enables the Private VLAN.
dis Disables the Private VLAN.
cur Displays current parameters for the selected Private VLAN.

/cfg/l3

Layer 3 Configuration Menu

```
[Layer 3 Menu]
     if       - Interface Menu
     gw       - Default Gateway Menu
     route    - Static Route Menu
     mroute   - Static IP Multicast Route Menu
     arp      - ARP Menu
     frwd     - Forwarding Menu
     nwf      - Network Filters Menu
     rmap     - Route Map Menu
     rip      - Routing Information Protocol Menu
     ospf     - Open Shortest Path First (OSPF) Menu
     bgp      - Border Gateway Protocol Menu
     mld      - MLD Menu
     igmp     - IGMP Menu
     ikev2    - IKEv2 Menu
     ipsec    - IPsec Menu
     dns      - Domain Name System Menu
     bootp    - Bootstrap Protocol Relay Menu
     vrrp     - Virtual Router Redundancy Protocol Menu
     gw6      - IP6 Default Gateway Menu
     route6   - Static IP6 Route Menu
     nbrcache - IP6 Static Neighbor Cache Menu
     ip6pmtu  - IP6 Path MTU Menu
     ospf3    - Open Shortest Path First v3 (OSPFv3) Menu
     ndprefix - IP6 Neighbor Discovery Prefix Menu
     ppt      - Prefix policy table Menu
     loopif   - Loopback Interface Menu
     rtrid    - Set router ID
     flooding - Flooding Unregistered IPMCs Menu
     cur      - Display current IP configuration
```

Table 249. Layer 3 Configuration Menu (/cfg/l3)

Command Syntax and Usage
`if` *<interface number (1-128>* Displays the IP Interface Menu. To view menu options, see page 312.
`gw` *<default gateway number (1-4>* Displays the IP Default Gateway Menu. To view menu options, see page 313.
`route` Displays the IP Static Route Menu. To view menu options, see page 315.
`mroute` Displays the Static IP Multicast Route Menu. To view menu options, see page 316.
`arp` Displays the Address Resolution Protocol Menu. To view menu options, see page 317.
`frwd` Displays the IP Forwarding Menu. To view menu options, see page 318.

Table 249. Layer 3 Configuration Menu (/cfg/l3) (continued)

Command Syntax and Usage
`nwf` *<network filter number (1-256)>* Displays the Network Filter Configuration Menu. To view menu options see page 319.
`rmap` *<route map number (1-32)>* Displays the Route Map Menu. To view menu options see page 320.
`rip` Displays the Routing Interface Protocol Menu. To view menu options, see page 323.
`ospf` Displays the OSPF Menu. To view menu options, see page 326.
`bgp` Displays the Border Gateway Protocol Menu. To view menu options, see page 338.
`mld` Displays the Multicast Listener Discovery Menu. To view menu options, see page 344.
`igmp` Displays the IGMP Menu. To view menu options, see page 346.
`ikev2` Displays the IKEv2 Menu. To view menu options, see page 357.
`ipsec` Displays the IPsec Menu. To view menu options, see page 360.
`dns` Displays the IP Domain Name System Menu. To view menu options, see page 369.
`bootp` Displays the Bootstrap Protocol Menu. To view menu options, see page 369.
`vrrp` Displays the Virtual Router Redundancy Configuration Menu. To view menu options, see page 372.
`gw6` *<gateway number (1, 3, 4)>* Displays the IPv6 Gateway Configuration Menu. To view menu options, see page 380.
`route6` Displays the IPv6 Routing Configuration Menu. To view menu options, see page 381.

Table 249. Layer 3 Configuration Menu (/cfg/l3) (continued)

Command Syntax and Usage
`nbrcache` Displays the IPv6 Neighbor Discovery Cache Configuration Menu. To view menu options, see page 382.
`ip6pmtu` Displays the IPv6 Path MTU menu. To view menu options, see page 383.
`ospf3` Displays the OSPFv3 Configuration Menu. To view menu options, see page 384.
`ndprefix` Displays the IPv6 Neighbor Discovery Prefix menu. To view menu options, see page 398.
`ppt` Displays the Prefix Policy Table menu. To view menu options, see page 401.
`loopif` Displays the IP Loopback Interface Menu. To view menu options, see page 402.
`rtrid` *<IP address (such as, 192.4.17.101)>* Sets the router ID.
`flooding` Displays the Flooding Configuration Menu. To view menu options, see page 403.
`cur` Displays the current IP configuration.

/cfg/l3/if <*interface number*>
IP Interface Configuration Menu

```
[IP Interface 1 Menu]
     addr     - Set IP address
     vlan     - Set VLAN number
     relay    - Enable/disable BOOTP relay
     ena      - Enable IP interface
     dis      - Disable IP interface
     del      - Delete IP interface
     cur      - Display current interface configuration
```

The CN4093 can be configured with up to 128 IP interfaces. Each IP interface represents the CN4093 on an IP subnet on your network. The Interface option is disabled by default.

IP interfaces 127 and 128 are reserved for switch management. If the IPv6 feature is enabled on the switch, IP interfaces 125 and 126 are also reserved.

Note: To maintain connectivity between the management module and the CN4093, use the management module interface to change the IP address of the switch.

Table 250. IP Interface Menu Options (/cfg/l3/if)

Command Syntax and Usage
`addr` *<IPv4 address (such as 192.4.17.101)>* Configures the IPv4 address of the switch interface, using dotted decimal notation.
`vlan` *<VLAN number>* Configures the VLAN number for this interface. Each interface can belong to only one VLAN. Each VLAN can contain multiple IPv4 interfaces.
`relay disable|enable` Enables or disables the BOOTP relay on this interface. The default setting is `enabled`.
`ena` Enables this IP interface.
`dis` Disables this IP interface.
`del` Removes this IP interface.
`cur` Displays the current interface settings.

/cfg/l3/gw <*gateway number*>
Default Gateway Configuration Menu

```
[Default gateway 1 Menu]
      addr    - Set IP address
      intr    - Set interval between ping attempts
      retry   - Set number of failed attempts to declare gateway DOWN
      arp     - Enable/disable ARP only health checks
      ena     - Enable default gateway
      dis     - Disable default gateway
      del     - Delete default gateway
      cur     - Display current default gateway configuration
```

The switch can be configured with up to 4 IPv4 gateways.

This option is disabled by default.

Table 251. Default Gateway Menu Options (/cfg/l3/gw)

Command Syntax and Usage
`addr` *<default gateway address (such as, 192.4.17.44)>* Configures the IP address of the default IP gateway using dotted decimal notation.
`intr` *<0-60 seconds>* The switch pings the default gateway to verify that it's up. The `intr` option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.
`retry` *<number of attempts (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.
`arp disable|enable` Enables or disables Address Resolution Protocol (ARP) health checks. The default value is `disabled`. The `arp` option does not apply to management gateways.
`ena` Enables the gateway for use.
`dis` Disables the gateway.
`del` Deletes the gateway from the configuration.
`cur` Displays the current gateway settings.

/cfg/l3/route

IPv4 Static Route Configuration Menu

```
[IP Static Route Menu]
     add      - Add static route
     rem      - Remove static route
     clear    - Clear static routes
     interval - Change ECMP route health check ping interval
     retries  - Change the number of retries for ECMP health check
     ecmphash - Choose ECMP hash mechanism sip/dipsip
     cur      - Display current static routes
```

Up to 128 IPv4 static routes can be configured.

Table 252. IP Static Route Configuration Menu Options (cfg/l3/route)

Command Syntax and Usage
`add` *<destination> <mask> <gateway>* [*<interface number>*] Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway address. Enter all addresses using dotted decimal notation. **Note**: You may add multiple routes with the same IP address, but with different gateways. These routes become Equal Cost Multipath (ECMP) routes. The maximum number of gateways for each destination is five (5).
`rem` *<destination> <mask>* [*<interface number>*] Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation. **Note**: The gateway IP address is optional. Include the gateway when you remove an ECMP route. If you do not include the gateway, then all ECMP paths for the route are deleted.
`clear` *<destination IP address>*|*<gateway IP address>*|`all` *<value>* Clears the selected IPv4 static routes. **Note**: Use the gateway IP address to clear a single gateway for an ECMP route.
`interval` *<1-60>* Configures the ping interval for ECMP health checks, in seconds. The default value is one second.
`retries` *<1-60>* Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is 3.
`ecmphash [sip][dipsip]` Configures ECMP route hashing parameters. You may choose one of the following parameters: – `sip`: Source IP address – `dipsip`: Destination IP address and source IP address
`cur` Displays the current IPv4 static routes.

/cfg/l3/mroute

IP Multicast Route Configuration Menu

```
[IPMC Static Route Menu]
     addport  - Add static IP Multicast route for port
     remport  - Remove static IP Multicast route for port
     addtrnk  - Add static IP Multicast route for trunk
     remtrnk  - Remove static IP Multicast route for trunk
     addkey   - Add static IP Multicast route for Lacp adminkey
     remkey   - Remove static IP Multicast route or Lacp adminkey
     cur      - Display current static IPMC route configuration
```

The following table describes the IP Multicast (IPMC) route menu options. Before you can add an IPMC route, IGMP must be turned on (`/cfg/l3/igmp on`), and IGMP Relay must be enabled (`/cfg/l3/igmp/relay ena`) or IGMP Snooping must be enabled (`/cfg/l3/igmp/snoop ena`).

Table 253. IPMC Route Configuration Options

Command Syntax and Usage
`addport` *<IPMC destination> <VLAN number> <port alias or number>* `primary|backup|host` *<virtual router ID>*`|none` Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member port. Indicate whether the route is used for a primary, backup, or host multicast router.
`remport` *<IPMC destination> <VLAN number> <port alias or number>* `primary|backup|host` *<virtual router ID>*`|none` Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.
`addtrnk` *<IPMC destination> <VLAN number> <trunk group number>* `primary|backup|host` *<virtual router ID>*`|none` Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member trunk group. Indicate whether the route is used for a primary, backup, or host multicast router.
`remtrnk` *<IPMC destination> <VLAN number> <trunk group number>* `primary|backup|host` *<virtual router ID>*`|none` Removes a static multicast route. The destination address, VLAN, and member trunk group of the route to remove must be specified.
`addkey` *<IPMC destination> <VLAN number> <LACP adminkey>* `primary|backup|host` *<virtual router ID>*`|none` Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and LACP adminkey. Indicate whether the route is used for a primary, backup, or host multicast router.
`remkey` *<IPMC destination> <VLAN number> <LACP adminkey>* `primary|backup|host` *<virtual router ID>*`|none` Removes a static multicast route. The destination address, VLAN, and LACP adminkey of the route to remove must be specified.
`cur` Displays the current IP multicast routes.

/cfg/l3/arp
ARP Configuration Menu

Address Resolution Protocol (ARP) is the TCP/IP protocol that resides within the Internet layer. ARP resolves a physical address from an IP address. ARP queries machines on the local network for their physical addresses. ARP also maintains IP to physical address pairs in its cache memory. In any IP communication, the ARP cache is consulted to see if the IP address of the computer or the router is present in the ARP cache. Then the corresponding physical address is used to send a packet.

```
[ARP Menu]
     static   - Static ARP Menu
     rearp    - Set re-ARP period in minutes
     cur      - Display current ARP configuration
```

Table 254. ARP Configuration Menu Options (/cfg/l3/arp)

Command Syntax and Usage
`static` Displays Static ARP menu. To view options, see page 317.
`rearp` *<2-120 minutes>* Defines re-ARP period, in minutes, for entries in the switch arp table. When ARP entries reach this value the switch will re-ARP for the address to attempt to refresh the ARP cache. The default value is 5 minutes.
`cur` Displays the current ARP configurations.

/cfg/l3/arp/static
ARP Static Configuration Menu

Static ARP entries are permanent in the ARP cache and do not age out like the ARP entries that are learned dynamically. Static ARP entries enable the switch to reach the hosts without sending an ARP broadcast request to the network. Static ARPs are also useful to communicate with devices that do not respond to ARP requests. Static ARPs can also be configured on some gateways as a protection against malicious ARP Cache corruption and possible DOS attacks.

```
[Static ARP Menu]
     add      - Add a permanent ARP entry
     del      - Delete an ARP entry
     clear    - Clear static ARP entries
     cur      - Display current static ARP configuration
```

Table 255. ARP Static Configuration Menu Options (/cfg/l3/arp/static)

Command Syntax and Usage
`add` *<IP address> <MAC address> <VLAN number> <port number>* Adds a permanent ARP entry.
`del` *<IP address (such as, 192.4.17.101)>* Deletes a permanent ARP entry.

`clear [all|if` *<interface number>*`|vlan` *<VLAN number>*`|`
`port` *<port number>*`]`
Clears static ARP entries.

`cur` Displays current static ARP configuration.

/cfg/l3/frwd
IP Forwarding Configuration Menu

```
[IP Forwarding Menu]
     dirbr    - Enable or disable forwarding directed broadcasts
     noicmprd - Enable/disable No ICMP Redirects
     icmp6rd  - Enable/disable ICMPv6 Redirects
     on       - Globally turn IP Forwarding ON
     off      - Globally turn IP Forwarding OFF
     cur      - Display current IP Forwarding configuration
```

Table 256. IP Forwarding Configuration Menu Options (/cfg/l3/frwd)

Command Syntax and Usage
`dirbr disable|enable` Enables or disables forwarding directed broadcasts. The default setting is `disabled`.
`noicmprd disable|enable` Enables or disables ICMP re-directs. The default setting is `disabled`.
`icmp6rd disable|enable` Enables or disables IPv6 ICMP re-directs. The default setting is `disabled`.
`on` Enables IP forwarding (routing) on the CN4093. Forwarding is turned on by default.
`off` Disables IP forwarding (routing) on the CN4093.
`cur` Displays the current IP forwarding settings.

/cfg/l3/nwf <1-256>
Network Filter Configuration Menu

```
[IP Network Filter 1 Menu]
      addr    - IP Address
      mask    - IP network filter mask
      enable  - Enable Network Filter
      disable - Disable Network Filter
      delete  - Delete Network Filter
      cur     - Display current Network Filter configuration
```

Table 257. IP Network Filter Menu Options (/cfg/l3/nwf)

Command Syntax and Usage
addr *<IP address, such as 192.4.17.44>* Sets the IP address that will be accepted by the peer when the filter is enabled. If used with the mask option, a range of IP addresses is accepted. The default address is 0.0.0.0 For Border Gateway Protocol (BGP), assign the network filter to an access-list in a route map, then assign the route map to the peer.
mask *<IP network filter mask>* Sets the network filter mask that is used with addr. The default value is 0.0.0.0 For Border Gateway Protocol (BGP), assign the network filter to a route map, then assign the route map to the peer.
enable Enables the Network Filter configuration.
disable Disables the Network Filter configuration.
delete Deletes the Network Filter configuration.
cur Displays the current the Network Filter configuration.

/cfg/l3/rmap <route map number>

Routing Map Configuration Menu

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

```
[IP Route Map 1 Menu]
      alist   - Access List number
      aspath  - AS Filter Menu
      ap      - Set as-path prepend of the matched route
      lp      - Set local-preference of the matched route
      metric  - Set metric of the matched route
      type    - Set OSPF metric-type of the matched route
      prec    - Set the precedence of this route map
      weight  - Set weight of the matched route
      enable  - Enable route map
      disable - Disable route map
      delete  - Delete route map
      cur     - Display current route map configuration
```

Routing maps control and modify routing information.

Table 258. Routing Map Menu Options (/cfg/l3/rmap)

Command Syntax and Usage
`alist` *<number 1-8>* Displays the Access List menu. For more information, see page 321.
`aspath` *<number 1-8>* Displays the Autonomous System (AS) Filter menu. For more information, see page 322.
`ap` *<AS number>* [*<AS number>*] [*<AS number>*]|`none` Sets the AS path preference of the matched route. You can configure up to three path preferences.
`lp` *<(0-4294967294)>*|`none` Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred.
`metric` *<(1-4294967294)>*|`none` Sets the metric of the matched route.
`type` *<value (1|2)>*|`none` Assigns the type of OSPF metric. The default is type 1. – Type 1—External routes are calculated using both internal and external metrics. – Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2. – `none`—Removes the OSPF metric.
`prec` *<value (1-255)>* Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.

Table 258. Routing Map Menu Options (/cfg/l3/rmap) (continued)

Command Syntax and Usage
`weight` *<value (0-65534)>*`|none` Sets the weight of the route map.
`enable` Enables the route map.
`disable` Disables the route map.
`delete` Deletes the route map.
`cur` Displays the current route configuration.

/cfg/l3/rmap *<route map number>*/alist *<access list number>*

IP Access List Configuration Menu

Note: The *route map number (*1-32) and the *access list number* (1-8) represent the IP access list you wish to configure.

```
[IP Access List 1 Menu]
      nwf     - Network Filter number
      metric  - Metric
      action  - Set Network Filter action
      enable  - Enable Access List
      disable - Disable Access List
      delete  - Delete Access List
      cur     - Display current Access List configuration
```

Table 259. IP Access List Menu Options (/cfg/l3/rmap/alist)

Command Syntax and Usage
`nwf` *<network filter number (1-256)>* Sets the network filter number. See "/cfg/l3/nwf <1-256>" on page 319 for details.
`metric` *<(1-4294967294)>*`|none` Sets the metric value in the AS-External (ASE) LSA.
`action permit|deny` Permits or denies action for the access list.
`enable` Enables the access list.
`disable` Disables the access list.

Table 259. IP Access List Menu Options (/cfg/l3/rmap/alist) (continued)

Command Syntax and Usage
`delete` Deletes the access list.
`cur` Displays the current Access List configuration.

/cfg/l3/rmap <*route map number*>/aspath <*autonomous system path*>

Autonomous System Filter Path Menu

Note: The *rmap number (*1-32) and the *path number* (1-8) represent the AS path you wish to configure.

```
[AS Filter 1 Menu]
      as      - AS number
      action  - Set AS Filter action
      enable  - Enable AS Filter
      disable - Disable AS Filter
      delete  - Delete AS Filter
      cur     - Display current AS Filter configuration
```

Table 260. AS Filter Menu Options (/cfg/l3/rmap/aspath)

Command Syntax and Usage
`as` *<AS number (1-65535)>* Sets the Autonomous System filter's path number.
`action` <*permit*|*deny (p*|*d)*> Permits or denies Autonomous System filter action.
`enable` Enables the Autonomous System filter.
`disable` Disables the Autonomous System filter.
`delete` Deletes the Autonomous System filter.
`cur` Displays the current Autonomous System filter configuration.

/cfg/l3/rip
Routing Information Protocol Configuration Menu

```
[Routing Information Protocol Menu]
     if       - RIP Interface Menu
     update   - Set update period in seconds
     on       - Globally turn RIP ON
     off      - Globally turn RIP OFF
     current  - Display current RIP configuration
```

The RIP Menu is used for configuring Routing Information Protocol (RIP) parameters. This option is turned off by default.

Table 261. RIP Menu Options (/cfg/l3/rip)

Command Syntax and Usage
`if` *<interface number>* Displays the RIP Interface menu. For more information, see page 323.
`update` *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.
`on` Globally turns RIP `on`.
`off` Globally turns RIP `off`.
`cur` Displays the current RIP configuration.

/cfg/l3/rip/if <*interface number*>
Routing Information Protocol Interface Configuration Menu

```
[RIP Interface 1 Menu]
     version  - Set RIP version
     supply   - Enable/disable supplying route updates
     listen   - Enable/disable listening to route updates
     poison   - Enable/disable poisoned reverse
     split    - Enable/disable split horizon
     trigg    - Enable/disable triggered updates
     mcast    - Enable/disable multicast updates
     default  - Set default route action
     metric   - Set metric
     auth     - Set authentication type
     key      - Set authentication key
     enable   - Enable interface
     disable  - Disable interface
     current  - Display current RIP interface configuration
```

The RIP Interface Menu is used for configuring Routing Information Protocol parameters for the selected interface.

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

Table 262. RIP Interface Menu Options (/cfg/l3/rip/if)

Command Syntax and Usage
`version 1|2|both` Configures the RIP version used by this interface. The default value is version `2`.
`supply disable|enable` When enabled, the switch supplies routes to other routers. The default value is `enabled`.
`listen disable|enable` When enabled, the switch learns routes from other routers. The default value is `enabled`.
`poison disable|enable` When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is `disabled`.
`split disable|enable` Enables or disables split horizon. The default value is `enabled`.
`trigg disable|enable` Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is `enabled`.
`mcast disable|enable` Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is `enabled`.
`default none|listen|supply|both` When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is `none`.
`metric` *<1-15>* Configures the route metric, which indicates the relative distance to the destination. The default value is `1`.
`auth none|password` Configures the authentication type. The default is `none`.
`key` *<password>*`|none` Configures the authentication key password.
`enable` Enables this RIP interface.

Table 262. RIP Interface Menu Options (/cfg/l3/rip/if) (continued)

Command Syntax and Usage
`disable` Disables this RIP interface.
`current` Displays the current RIP configuration.

/cfg/l3/ospf

Open Shortest Path First Configuration Menu

```
[Open Shortest Path First Menu]
      aindex  - OSPF Area (index) menu
      range   - OSPF Summary Range menu
      if      - OSPF Interface menu
      loopif  - OSPF Loopback Interface Menu
      virt    - OSPF Virtual Links menu
      md5key  - OSPF MD5 Key Menu
      host    - OSPF Host Entry menu
      redist  - OSPF Route Redistribute menu
      lsdb    - Set the LSDB limit
      default - Originate default route information
      on      - Globally turn OSPF ON
      off     - Globally turn OSPF OFF
      cur     - Display current OSPF configuration
```

Table 263. OSPF Configuration Menu (/cfg/l3/ospf)

Command Syntax and Usage
`aindex` *<area index (0-2)>* Displays the Area Index menu. This area index does not represent the actual OSPF area number. See page 328 to view menu options.
`range` *<1-16>* Displays the Summary Range menu. See page 329 to view menu options.
`if` *<interface number>* Displays the OSPF Interface configuration menu. See page 331 to view menu options.
`loopif` *<1-5>* Displays the OSPF Loopback Interface configuration menu. See page 332 to view menu options.
`virt` *<virtual link (1-3)>* Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See page 334 to view menu options.
`md5key` *<key ID (1-255)>* Assigns a string to MD5 authentication key.
`host` *<1-128>* Displays the menu for configuring OSPF for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 335 to view menu options.
`redist fixed|static|rip|ebgp|ibgp` Displays Route Distribution menu. See page 336 to view menu options.
`lsdb` *<LSDB limit (0-2048, 0 for no limit)>* Sets the link state database limit.

Table 263. OSPF Configuration Menu (/cfg/l3/ospf) (continued)

Command Syntax and Usage
`default` *<metric (1-16777214)> <metric-type 1|2>*`|none` Sets one default route among multiple choices in an area. Use `none` for no default.
`on` Enables OSPF on the CN4093.
`off` Disables OSPF on the CN4093.
`cur` Displays the current OSPF configuration settings.

/cfg/l3/ospf/aindex <*area index*>

Area Index Configuration Menu

```
[OSPF Area (index) 1 Menu]
      areaid  - Set area ID
      type    - Set area type
      metric  - Set stub area metric
      auth    - Set authentication type
      spf     - Set time interval between two SPF calculations
      enable  - Enable area
      disable - Disable area
      delete  - Delete area
      cur     - Display current OSPF area configuration
```

Table 264. Area Index Configuration Menu Options (/cfg/l3/ospf/aindex)

Command Syntax and Usage
areaid <*IP address (such as, 192.4.17.101)*> Defines the IP address of the OSPF area number.
type transit|stub|nssa Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. **Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. **NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.
metric <*metric value (1-65535)*> Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions. Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.
auth none|password|md5 – none: No authentication required. – password: Authenticates simple passwords so that only trusted routing devices can participate. – md5: This parameter is used when MD5 cryptographic authentication is required.

Table 264. Area Index Configuration Menu Options (/cfg/l3/ospf/aindex) (continued)

Command Syntax and Usage
`spf` *<interval (1-255)>* Configures the minimum time interval, in seconds, between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm. The default value is 10 seconds.
`enable` Enables the OSPF area.
`disable` Disables the OSPF area.
`delete` Deletes the OSPF area.
`cur` Displays the current OSPF configuration.

/cfg/l3/ospf/range *<range number>*
OSPF Summary Range Configuration Menu

```
[OSPF Summary Range 1 Menu]
      addr    - Set IP address
      mask    - Set IP mask
      aindex  - Set area index
      hide    - Enable/disable hide range
      enable  - Enable range
      disable - Disable range
      delete  - Delete range
      cur     - Display current OSPF summary range configuration
```

Table 265. OSPF Summary Range Configuration Menu Options (/cfg/l3/ospf/range)

Command Syntax and Usage
`addr` *<IP Address (such as, 192.4.17.101)>* Configures the base IP address for the range.
`mask` *<IP mask (such as, 255.255.255.0)>* Configures the IP address mask for the range.
`aindex` *<area index (0-2)>* Configures the area index used by the CN4093.
`hide disable|enable` Hides the OSPF summary range.
`enable` Enables the OSPF summary range.
`disable` Disables the OSPF summary range.

Table 265. OSPF Summary Range Configuration Menu Options (/cfg/l3/ospf/range)

Command Syntax and Usage
`delete` Deletes the OSPF summary range.
`cur` Displays the current OSPF summary range.

/cfg/l3/ospf/if <*interface number*>

OSPF Interface Configuration Menu

```
[OSPF Interface 1 Menu]
      aindex  - Set area index
      prio    - Set interface router priority
      cost    - Set interface cost
      hello   - Set hello interval in seconds or milliseconds
      dead    - Set dead interval in seconds or milliseconds
      trans   - Set transit delay in seconds
      retra   - Set retransmit interval in seconds
      key     - Set authentication key
      mdkey   - Set MD5 key ID
      passive - Enable/disable passive interface
      ptop    - Enable/disable point-to-point interface
      enable  - Enable interface
      disable - Disable interface
      delete  - Delete interface
      cur     - Display current OSPF interface configuration
```

Table 266. OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)

Command Syntax and Usage
aindex <*area index (0-2)*> Configures the OSPF area index.
prio <*priority value (0-255)*> Configures the priority value for the CN4093's OSPF interfaces. (A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)
cost <*1-65535*> Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.
hello <*1-65535*> hello <*50-65535ms*> Configures the interval, in seconds or milliseconds, between the hello packets for the interfaces.
dead <*1-65535*> dead <*1000-65535ms*> Configures the health parameters of a hello packet, in seconds or milliseconds, before declaring a silent router to be down.
trans <*1-3600*> Configures the transit delay in seconds.
retra <*1-3600*> Configures the retransmit interval in seconds.
key <*key*>|none Sets the authentication key to clear the password.

Table 266. OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if) (continued)

Command Syntax and Usage
mdkey *<key ID (1-255)>*|none Assigns an MD5 key to the interface.
passive enable|disable Sets the interface as passive. On a passive interface, you can disable OSPF protocol exchanges, but the router advertises the interface in its LSAs so that IP connectivity to the attached network segment will be established.
ptop enable|disable Sets the interface as point-to-point.
enable Enables OSPF interface.
disable Disables OSPF interface.
delete Deletes OSPF interface.
cur Displays the current settings for OSPF interface.

/cfg/l3/ospf/loopback *<1-5>*

OSPF Loopback Interface Configuration Menu

```
[OSPF Loopback Interface 1  Menu]
     aindex   - Set area index
     enable   - Enable interface
     disable  - Disable interface
     delete   - Delete interface
     cur      - Display current OSPF interface configuration
```

Table 267. OSPF Loopback Interface Configuration Options (/cfg/l3/ospf/loopif)

Command Syntax and Usage
aindex *<area index (0-2)>* Configures the area index used by the loopback interface.
enable Enables the loopback interface.
disable Disables the loopback interface.

Table 267. OSPF Loopback Interface Configuration Options (/cfg/l3/ospf/loopif) (continued)

Command Syntax and Usage
`delete` Deletes the OSPF loopback interface.
`cur` Displays the current parameters for the OSPF loopback interface.

/cfg/l3/ospf/virt <*link number*>

OSPF Virtual Link Configuration Menu

```
[OSPF Virtual Link 1 Menu]
      aindex  - Set area index
      hello   - Set hello interval in seconds or milliseconds
      dead    - Set dead interval in seconds or milliseconds
      trans   - Set transit delay in seconds
      retra   - Set retransmit interval in seconds
      nbr     - Set router ID of virtual neighbor
      key     - Set authentication key
      mdkey   - Set MD5 key ID
      enable  - Enable interface
      disable - Disable interface
      delete  - Delete interface
      cur     - Display current OSPF interface configuration
```

Table 268. OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt)

Command Syntax and Usage
aindex <*area index (0-2)*> Configures the OSPF area index.
hello <*1-65535*> hello <*50-65535ms*> Configures the authentication parameters of a hello packet, in seconds or milliseconds. The default value is 10 seconds.
dead <*1-65535*> dead <*1000-65535ms*> Configures the health parameters of a hello packet, in seconds or milliseconds. The default value is 60 seconds.
trans <*1-3600*> Configures the delay in transit, in seconds. The default value is one second.
retra <*1-3600*> Configures the retransmit interval, in seconds. The default value is five seconds.
nbr <*NBR router ID (IP address)*> Configures the router ID of the virtual neighbor. The default value is 0.0.0.0.
key <*password*>|none Configures the password (up to eight characters) for each virtual link. The default value is none.
mdkey <*key ID (1-255)*>|none Sets MD5 key ID for each virtual link. The default value is none.
enable Enables OSPF virtual link.
disable Disables OSPF virtual link.

Table 268. OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt) (continued)

Command Syntax and Usage
`delete` Deletes OSPF virtual link.
`cur` Displays the current OSPF virtual link settings.

/cfg/l3/ospf/host <*host number*>

OSPF Host Entry Configuration Menu

```
[OSPF Host Entry 1 Menu]
      addr    - Set host entry IP address
      aindex  - Set area index
      cost    - Set cost of this host entry
      enable  - Enable host entry
      disable - Disable host entry
      delete  - Delete host entry
      cur     - Display current OSPF host entry configuration
```

Table 269. OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)

Command Syntax and Usage
`addr` *<IP address (such as, 192.4.17.101)>* Configures the base IP address for the host entry.
`aindex` *<area index (0-2)>* Configures the area index of the host.
`cost` *<1-65535>* Configures the cost value of the host.
`enable` Enables OSPF host entry.
`disable` Disables OSPF host entry.
`delete` Deletes OSPF host entry.
`cur` Displays the current OSPF host entries.

/cfg/l3/ospf/redist fixed|static|rip|ebgp|ibgp

OSPF Route Redistribution Configuration Menu

```
[OSPF Redistribute Fixed Menu]
      add     - Add rmap into route redistribution list
      rem     - Remove rmap from route redistribution list
      export  - Export all routes of this protocol
      cur     - Display current route-maps added
```

Table 270. OSPF Route Redistribution Menu Options (/cfg/l3/ospf/redist)

Command Syntax and Usage
add *(<route map (1-32)> <route map (1-32)>...* |all Adds selected routing maps to the rmap list.To add all the 32 route maps, enter all. To add specific route maps, enter routing map numbers one per line, NULL at the end. This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem *(<route map (1-32)> <route map (1-32)> ...* |all Removes the route map from the route redistribution list. Removes routing maps from the rmap list. To remove all 32 route maps, enter all. To remove specific route maps, enter routing map numbers one per line, NULL at end.
export *<metric (1-16777214)> <metric type (1-2)>* |none Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none.
cur Displays the current route map settings.

/cfg/l3/ospf/md5key <*key ID*>

OSPF MD5 Key Configuration Menu

```
[OSPF MD5 Key 1 Menu]
      key     - Set authentication key
      delete  - Delete key
      cur     - Display current MD5 key configuration
```

Table 271. OSPF MD5 Key Configuration Menu Options (/cfg/ip/ospf/md5key)

Command Syntax and Usage
`key` <*1-16 characters*> Sets the authentication key for this OSPF packet.
`delete` Deletes the authentication key for this OSPF packet.
`cur` Displays the current MD5 key configuration.

/cfg/l3/bgp

Border Gateway Protocol Configuration Menu

```
[Border Gateway Protocol Menu]
      peer    - Peer menu
      aggr    - Aggregation menu
      as      - Set Autonomous System (AS) number
      pref    - Set Local Preference
      on      - Globally turn BGP ON
      off     - Globally turn BGP OFF
      cur     - Display current BGP configuration
```

Border Gateway Protocol (BGP) is an Internet protocol that enables routers on a network to share routing information with each other and advertise information about the segments of the IP address space they can access within their network with routers on external networks. BGP allows you to decide what is the “best” route for a packet to take from your network to a destination on another network, rather than simply setting a default route from your border router(s) to your upstream provider(s). You can configure BGP either within an autonomous system or between different autonomous systems. When run within an autonomous system, it's called internal BGP (iBGP). When run between different autonomous systems, it's called external BGP (eBGP). BGP is defined in RFC 1771.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current IBM Networking OS implementation, the CN4093 does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

Note: Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 272. Border Gateway Protocol Menu (/cfg/l3/bgp)

Command Syntax and Usage
`peer` *<peer number (1-12)>* Displays the menu used to configure each BGP *peer.* Each border router, within an autonomous system, exchanges routing information with routers on other external networks. To view menu options, see page 339.
`aggr` *<aggregate number (1-16)>* Displays the Aggregation Menu. To view menu options, see page 343.
`as` *<0-65535>* Set Autonomous System number.
`pref` *<local preference (0-4294967294)>* Sets the local preference. The path with the higher value is preferred. When multiple peers advertise the same route, use the route with the shortest AS path as the preferred route if you are using eBGP, or use the local preference if you are using iBGP.
`on` Globally turns BGP on.

Table 272. Border Gateway Protocol Menu (/cfg/l3/bgp) (continued)

Command Syntax and Usage
`off` Globally turns BGP off.
`cur` Displays the current BGP configuration.

/cfg/l3/bgp/peer <*peer number*>
BGP Peer Configuration Menu

```
[BGP Peer 1 Menu]
      redist   - Redistribution menu
      addr     - Set remote IP address
      ras      - Set remote autonomous system number
      usrc     - Set local IP interface
      uloopsrc - Set local IP loopback interface
      hold     - Set hold time
      alive    - Set keep alive time
      advert   - Set min time between advertisements
      retry    - Set connect retry interval
      orig     - Set min time between route originations
      ttl      - Set time-to-live of IP datagrams
      addi     - Add rmap into in-rmap list
      addo     - Add rmap into out-rmap list
      remi     - Remove rmap from in-rmap list
      remo     - Remove rmap from out-rmap list
      enable   - Enable peer
      disable  - Disable peer
      delete   - Delete peer
      passwd   - Set password
      passive  - Enable/disable BGP passive mode
      cur      - Display current peer configuration
```

This menu is used to configure BGP peers, which are border routers that exchange routing information with routers on internal and external networks. The peer option is disabled by default.

Table 273. BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer)

Command Syntax and Usage
`redist` Displays BGP Redistribution Menu. To view the menu options, see page 341.
`addr` *<IP address (such as 192.4.17.101)>* Defines the IP address for the specified peer (border router), using dotted decimal notation. The default address is 0.0.0.0.
`ras` *<AS number (0-65535)>* Sets the remote autonomous system number for the specified peer.
`usrc` *<interface number>* Sets the local IP interface for this peer.

Table 273. BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer) (continued)

Command Syntax and Usage
`uloopsrc` *<1-5>* Sets the loopback interface number for this peer.
`hold` *<hold time (0, 3-65535)>* Sets the period of time, in seconds, that will elapse before the peer session is torn down because the switch hasn't received a "keep alive" message from the peer. The default value is 180.
`alive` *<keep-alive time (0, 1-21845)>* Sets the keep-alive time for the specified peer in seconds. The default value is 60.
`advert` *<min adv time (1-65535)>* Sets time, in seconds, between advertisements. The default value is 60 seconds.
`retry` *<connect retry interval (1-65535)>* Sets connection retry interval, in seconds. The default value is 120 seconds.
`orig` *<min orig time (1-65535)>* Sets the minimum time between route originations, in seconds. The default value is 15 seconds.
`ttl` *<number of router hops (1-255)>* Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. TTL specifies a certain time span in seconds that, when exhausted, would cause the packet to be discarded. The TTL is determined by the number of router hops the packet is allowed before it must be discarded. This command specifies the number of router hops that the IP packet can make. This value is used to restrict the number of "hops" the advertisement makes. It is also used to support multi-hops, which allow BGP peers to talk across a routed network. The default number is set at 1. **Note:** The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).
`addi` *<route map ID (1-32)>* Adds route map into in-route map list.
`addo` *<route map ID (1-32)>* Adds route map into out-route map list.
`remi` *<route map ID (1-32)>* Removes route map from in-route map list.
`remo` *<route map ID (1-32)>* Removes route map from out-route map list.
`enable` Enables this peer configuration.

Table 273. BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer) (continued)

Command Syntax and Usage
`disable` Disables this peer configuration.
`delete` Deletes this peer configuration.
`passwd <1-16 characters>|none` Configures the BGP peer password.
`passive enable|disable` Enables or disables BGP passive mode, which prevents the switch from initiating BGP connections with peers. Instead, the switch waits for the peer to send an open message first.
`cur` Displays the current BGP peer configuration.

/cfg/l3/bgp/peer/redist
BGP Redistribution Configuration Menu

```
[Redistribution Menu]
      metric  - Set default-metric of advertised routes
      default - Set default route action
      rip     - Enable/disable advertising RIP routes
      ospf    - Enable/disable advertising OSPF routes
      fixed   - Enable/disable advertising fixed routes
      static  - Enable/disable advertising static routes
      cur     - Display current redistribution configuration
```

Table 274. BGP Redistribution Menu Options (/cfg/l3/bgp/peer/redist)

Command Syntax and Usage
`metric <metric (1-4294967294)>|none` Sets default metric of advertised routes.
`default none|import|originate|redistribute` Sets default route action. Default routes can be configured as follows: – `none`: No routes are configured – `import`: Import these routes. – `originate`: The switch sends a default route to peers if it does not have any default routes in its routing table. – `redistribute`: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol in this redistribute submenu.

Table 274. BGP Redistribution Menu Options (/cfg/l3/bgp/peer/redist) (continued)

Command Syntax and Usage
`rip disable|enable` Enables or disables advertising RIP routes
`ospf disable|enable` Enables or disables advertising OSPF routes.
`fixed disable|enable` Enables or disables advertising fixed routes.
`static disable|enable` Enables or disables advertising static routes.
`cur` Displays current redistribution configuration.

/cfg/l3/bgp/aggr <*aggregation number*>

BGP Aggregation Configuration Menu

```
[BGP Aggr 1 Menu]
      addr    - Set aggregation IP address
      mask    - Set aggregation network mask
      enable  - Enable aggregation
      disable - Disable aggregation
      delete  - Delete aggregation
      cur     - Display current aggregation configuration
```

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

Table 275. BGP Aggregation Configuration Menu Options (/cfg/l3/bgp/aggr)

Command Syntax and Usage
addr <*IP address (such as 192.4.17.101)*> Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.
mask <*IP subnet mask (such as, 255.255.255.0)*> This IP address mask is used with addr to define the range of IP addresses that will be accepted by the peer when the aggregation is enabled. The default address is 0.0.0.0.
ena Enables this BGP aggregation.
dis Disables this BGP aggregation.
del Deletes this BGP aggregation.
cur Displays the current BGP aggregation configuration.

/cfg/l3/mld
MLD Configuration Menu

```
[MLD Menu]
     if       - MLD Interface Menu
     on       - Globally turn MLD ON
     off      - Globally turn MLD OFF
     default  - Set default configuration
     cur      - Display current MLD configuration
```

Table 276 describes the commands used to configure basic Multicast Listener Discovery parameters.

Table 276. MLD Menu Options (/cfg/l3/mld)

Command Syntax and Usage
`if` *<interface number>* Displays the MLD Interface Menu. To view menu options, see page 345.
`on` Globally turns MLD on.
`off` Globally turns MLD off.
`default` Resets MLD parameters to their default values.
`cur` Displays the current MLD configuration parameters.

/cfg/l3/mld/if <*interface number*>

MLD Interface Configuration Menu

```
[MLD Interface 1 Menu]
     version  - Set Multicast Listener Discovery protocol version
     robust   - Set MLD robustness
     qintrval - Set MLD query interval
     llistnr  - Set MLD last listener query interval
     qri      - Set MLD query response interval
     dmrtr    - Enable/disable dynamic Mrouter learning on interface
     ena      - Enable MLD on interface
     dis      - Disable MLD on interface
     default  - Set MLD settings to factory default
     cur      - Display current MLD configuration for this interface
```

Table 277 describes the commands used to configure Multicast Listener Discovery parameters for an interface.

Table 277. MLD Interface Menu Options (/cfg/l3/mld/if)

Command Syntax and Usage
`version` <*1-2*> Defines the MLD protocol version number.
`robust` <*2-10*> Configures the MLD Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.
`qintrval` <*2-65535*> Configures the interval for MLD Query messages. The default value is 125 seconds.
`llistnr` <*1-32*> Configures the query interval for the Querier to send a query after receiving a host done message from a host on the subnet. The default value is 1 second.
`qri` <*1000-65535*> Configures the maximum response delay for MLD General Queries. This can be used to tune the burstiness of MLD messages on the link. The default value is 10,000 milliseconds.
`dmrtr enable|disable` Enables or disables dynamic Mrouter learning on the interface. The default setting is disabled.
`ena` Enables this MLD interface.
`dis` Disables this MLD interface.

Table 277. MLD Interface Menu Options (/cfg/l3/mld/if) (continued)

Command Syntax and Usage
`default` Resets MLD parameters for the selected interface to their default values.
`cur` Displays the current MLD interface configuration.

/cfg/l3/igmp
IGMP Configuration Menu

```
[IGMP Menu]
     snoop    - IGMP Snoop Menu
     relay    - IGMP Relay Menu
     mrouter  - Static Multicast Router Menu
     igmpflt  - IGMP Filtering Menu
     adv      - IGMP Advanced Menu
     querier  - IGMP Querier Menu
     on       - Globally turn IGMP ON
     off      - Globally turn IGMP OFF
     cur      - Display current IGMP configuration
```

Table 278 describes the commands used to configure basic IGMP parameters.

Table 278. IGMP Menu Options (/cfg/l3/igmp)

Command Syntax and Usage
`snoop` Displays the IGMP Snoop Menu. To view menu options, see page 347.
`relay` Displays the IGMP Relay Menu. To view menu options, see page 349.
`mrouter` Displays the Static Multicast Router Menu. To view menu options, see page 351.
`igmpflt` Displays the IGMP Filtering Menu. To view menu options, see page 352.
`adv` Displays the IGMP Advanced Menu. To view menu options, see page 354.
`querier` Displays the IGMP Querier Menu. To view menu options, see page 355.
`on` Globally turns IGMP on.

Table 278. IGMP Menu Options (/cfg/l3/igmp) (continued)

Command Syntax and Usage
`off` Globally turns IGMP off.
`cur` Displays the current IGMP configuration parameters.

/cfg/l3/igmp/snoop
IGMP Snooping Configuration Menu

```
[IGMP Snoop Menu]
      igmpv3  - IGMP Version3 Snoop Menu
      mrto    - Set multicast router timeout
      aggr    - Aggregate IGMP report
      srcip   - Set source ip to use when proxying GSQ
      add     - Add VLAN(s) to IGMP Snooping
      rem     - Remove VLAN(s) from IGMP Snooping
      clear   - Remove all VLAN(s) from IGMP Snooping
      ena     - Enable IGMP Snooping
      dis     - Disable IGMP Snooping
      def     - Set IGMP Snooping settings to factory default
      cur     - Display current 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 279 describes the commands used to configure IGMP Snooping.

Table 279. IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage
`igmpv3` Displays the IGMP version 3 Menu. To view menu options, see page 348.
`mrto` *<1-600 seconds>* 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.
`aggr enable|disable` Enables or disables IGMP Membership Report aggregation.
`srcip` *<IP address (such as, 192.4.17.101)>* Configures the source IP address used as a proxy for IGMP Group Specific Queries.
`add` *<VLAN number>* Adds the selected VLAN(s) to IGMP Snooping.

Table 279. IGMP Snoop Menu Options (/cfg/l3/igmp/snoop) (continued)

Command Syntax and Usage
`rem` *<VLAN number>* Removes the selected VLAN(s) from IGMP Snooping.
`clear` Removes all VLANs from IGMP Snooping.
`ena` Enables IGMP Snooping.
`dis` Disables IGMP Snooping.
`def` Resets IGMP Snooping parameters to their default values.
`cur` Displays the current IGMP Snooping parameters.

/cfg/l3/igmp/snoop/igmpv3

IGMP Version 3 Configuration Menu

```
[IGMP V3 Snoop Menu]
     sources  - Set the number of sources to snoop in group record
     v1v2     - Enable/disable snooping IGMPv1/v2 reports
     exclude  - Enable/disable snooping EXCLUDE mode reports
     ena      - Enable IGMPv3 Snooping
     dis      - Disable IGMPv3 Snooping
     cur      - Display current IGMP Snooping V3 configuration
```

Table 280 describes the commands used to configure IGMP version 3.

Table 280. IGMPv3 Menu Options (/cfg/l3/igmp/snoop/igmpv3)

Command Syntax and Usage
`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.
`v1v2 enable|disable` 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`.
`exclude enable|disable` Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is `enabled`.

Table 280. IGMPv3 Menu Options (/cfg/l3/igmp/snoop/igmpv3) (continued)

Command Syntax and Usage
`ena` Enables IGMP version 3. The default value is `disabled`.
`dis` Disables IGMP version 3.
`cur` Displays the current IGMP version 3 configuration.

/cfg/l3/igmp/relay
IGMP Relay Configuration Menu

```
[IGMP Relay Menu]
     mrtr     - Upstream Multicast Router Menu
     add      - Add VLAN(s) to downstream
     rem      - Remove VLAN(s) from downstream
     clear    - Remove all VLAN(s) from downstream
     report   - Set unsolicited report interval
     ena      - Enable IGMP Relay
     dis      - Disable IGMP Relay
     def      - Set IGMP Relay settings to factory default
     cur      - Display current IGMP Relay configuration
```

Table 281 describes the commands used to configure IGMP Relay.

Table 281. IGMP Relay Menu Options (/cfg/l3/igmp/relay)

Command Syntax and Usage
`mrtr` *<multicast router number (1-2)>* Displays the Upstream Multicast Router Menu. To view menu options, see page 350.
`add` *<VLAN number>* Adds the VLAN to the list of IGMP Relay VLANs.
`rem` *<VLAN number>* Removes the VLAN from the list of IGMP Relay VLANs.
`clear` Removes all VLANs from the list of IGMP Relay VLANs.
`report` *<10-150>* Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10.
`ena` Enables IGMP Relay.

Table 281. IGMP Relay Menu Options (/cfg/l3/igmp/relay) (continued)

Command Syntax and Usage
`dis` Disables IGMP Relay.
`def` Resets IGMP Relay settings.
`cur` Displays the current IGMP Relay configuration.

/cfg/l3/igmp/relay/mrtr <*Mrouter number*>
IGMP Relay Multicast Router Configuration Menu

```
[Multicast router 2 Menu]
    addr     - Set IP address of multicast router
    intr     - Set interval between ping attempts
    retry    - Set number of failed attempts to declare router DOWN
    restr    - Set number of successful attempts to declare router UP
    version  - Set IGMP version
    ena      - Enable multicast router
    dis      - Disable multicast router
    del      - Delete multicast router
    cur      - Display current multicast router configuration
```

Table 282 describes the commands used to configure the IGMP Relay multicast router.

Table 282. IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr)

Command Syntax and Usage
`addr` <*IP address (such as, 224.0.1.0)*> Configures the IP address of the IGMP multicast router used for IGMP Relay.
`intr` <*1-60*> Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.
`retry` <*1-120*> Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4.
`restr` <*1-128*> Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5.
`version` <*1-2*> Configures the IGMP version (1 or 2) of the multicast router.

Table 282. IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr) (continued)

Command Syntax and Usage
`ena` Enables the multicast router.
`dis` Disables the multicast router.
`del` Deletes the multicast router from IGMP Relay.
`cur` Displays the current IGMP Relay multicast router parameters.

/cfg/l3/igmp/mrouter
IGMP Static Multicast Router Configuration Menu

```
[Static Multicast Router Menu]
      add     - Add port as Multicast Router Port
      rem     - Remove port as Multicast Router Port
      clear   - Remove all Static Multicast Router Ports
      cur     - Display current Multicast Router configuration
```

Table 283 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 283. IGMP Static Multicast Router Menu Options (/cfg/l3/igmp/mrouter)

Command Syntax and Usage
`add` *<port number> <VLAN number> <IGMP version number>* 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.
`rem` *<port number> <VLAN number> <IGMP version number>* Removes a static multicast router from the selected port/VLAN combination.
`clear` Clears all static multicast routers from the switch.
`cur` Displays the current IGMP Static Multicast Router parameters.

/cfg/l3/igmp/igmpflt
IGMP Filtering Configuration Menu

```
[IGMP Filter Menu]
      filter  - IGMP Filter Definition Menu
      port    - IGMP Filtering Port Menu
      ena     - Enable IGMP Filtering
      dis     - Disable IGMP Filtering
      cur     - Display current IGMP Filtering configuration
```

Table 284 describes the commands used to configure an IGMP filter.

Table 284. IGMP Filtering Menu Options (/cfg/l3/igmp/igmpflt)

Command Syntax and Usage
`filter` *<filter number (1-16)>* Displays the IGMP Filter Definition Menu. To view menu options, see page 353.
`port` *<port alias or number>* Displays the IGMP Filtering Port Menu. To view menu options, see page 354.
`ena` Enables IGMP filtering globally.
`dis` Disables IGMP filtering globally.
`cur` Displays the current IGMP Filtering parameters.

/cfg/l3/igmp/igmpflt/filter <*filter number*>

IGMP Filter Definition Menu

```
[IGMP Filter 1 Definition Menu]
      range   - Set IP Multicast address range
      action  - Set filter action
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current IGMP filter configuration
```

Table 285 describes the commands used to define an IGMP filter.

Table 285. IGMP Filter Definition Menu Options (/cfg/l3/igmp/igmpflt/filter)

Command Syntax and Usage
`range` *<IP multicast address (such as 225.0.0.10)> <IP multicast address>* Configures the range of IP multicast addresses for this filter.
`action allow|deny` Allows or denies multicast traffic for the IP multicast addresses specified. The default action is `deny`.
`ena` Enables this IGMP filter.
`dis` Disables this IGMP filter.
`del` Deletes this filter's parameter definitions.
`cur` Displays the current IGMP filter.

/cfg/l3/igmp/igmpflt/port <*port number*>

IGMP Filtering Port Configuration Menu

```
[IGMP Port EXT1 Menu]
      filt    - Enable/disable IGMP filtering on port
      add     - Add IGMP filter to port
      rem     - Remove IGMP filter from port
      cur     - Display current IGMP filtering Port configuration
```

Table 286 describes the commands used to configure a port for IGMP filtering.

Table 286. IGMP Filter Port Menu Options (/cfg/l3/igmp/igmpflt/port)

Command Syntax and Usage
`filt enable|disable` Enables or disables IGMP filtering on this port.
`add` *<filter number (1-16)>* Adds an IGMP filter to this port.
`rem` *<filter number (1-16)>* Removes an IGMP filter from this port.
`cur` Displays the current IGMP filter parameters for this port.

/cfg/l3/igmp/adv

IGMP Advanced Configuration Menu

```
[IGMP Advanced Menu]
     qintrval - Set IGMP query interval
     robust   - Set expected packet loss on subnet
     timeout  - Set report timeout
     fastlv   - Enable/disable Fastleave processing in VLAN
     rtralert - Send IGMP messages with Router Alert option
     cur      - Display current IGMP Advanced configuration
```

Table 287 describes the commands used to configure advanced IGMP parameters.

Table 287. IGMP Advanced Menu Options (/cfg/l3/igmp/adv)

Command Syntax and Usage
`qinterval` *<1-600>* Configures the interval for IGMP Query Reports. The default value is 125 seconds.
`robust` *<2-10>* Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.

Table 287. IGMP Advanced Menu Options (/cfg/l3/igmp/adv) (continued)

Command Syntax and Usage
`timeout <1-255>` Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.
`fastlv <VLAN number> disable|enable` Enables or disables Fastleave processing. Fastleave allows the switch to 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.
`retralert ena|dis` Enables or disables the Router Alert option in IGMP messages.
`cur` Displays the current IGMP Advanced parameters.

/cfg/l3/igmp/querier
IGMP Querier Configuration

```
[IGMP Querier Menu]
     ena      - Enable IGMP Querier
     dis      - Disable IGMP Querier
     vlan     - IGMP Querier vlan Menu
     cur      - Display IGMP Querier configuration
```

Table 288 describes the commands used to configure IGMP Querier.

Table 288. IGMP Querier Options

Command Syntax and Usage
`ena` Enables IGMP Querier.
`dis` Disables IGMP Querier.
`vlan <VLAN number>` Displays the IGMP Querier VLAN menu. To view menu options, see page 356.
`cur` Displays the current IGMP Querier parameters.

/cfg/l3/igmp/querier/vlan <*VLAN number*>

IGMP Querier VLAN Configuration

```
[IGMP Querier VLAN 1 Menu]
     type     - Set IGMP querier type
     time     - Set Queriers max response time
     interval - Set IGMP querier interval
     robust   - Set Queriers robustness
     srcip    - Set source IP to be used for IGMP
     count    - Set startup count for IGMP
     sinter   - Set startup query interval for IGMP
     version  - Sets the operating version of the IGMP snooping switch
     on       - Globally turn IGMP Querier ON
     off      - Globally turn IGMP Querier OFF
     default  - Set IGMP Querier settings to factory default
     cur      - Display current IGMP Querier configuration
```

Table 289 describes the commands used to configure IGMP Querier.

Table 289. IGMP Querier Options

Command Syntax and Usage
`type {ipv4|mac}` Sets the IGMP Querier election criteria as IPv4 address or Mac address. The default setting is `IPv4`.
`time` <*1-256*> Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100. By varying the Query Response Interval, an administrator may tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval.
`interval` <*1-608*> Configures the interval between IGMP Query broadcasts. The default value is 125 seconds.
`robust` <*2-10*> Configures the IGMP Robustness variable, which is the number of times that the switch sends each IGMP message. The default value is 2.
`srcip` <*IP address*> Configures the IGMP snooping source IP address for the selected VLAN.
`count` <*1-10*> Configures the Startup Query Count, which is the number of IGMP Queries sent out at startup. Each Query is separated by the Startup Query Interval. The default value is 2.
`sinter` <*1-608*> Configures the Startup Query Interval, which is the interval between General Queries sent out at startup.
`version {v1|v2|v3}` Configures the IGMP version. The default version is `v3`.

Table 289. IGMP Querier Options (continued)

Command Syntax and Usage
`on` Enables IGMP Querier on the selected VLAN.
`off` Disables IGMP Querier on the selected VLAN.
`default` Resets IGMP Querier parameters to default values.
`cur` Displays the current IGMP Querier VLAN parameters.

/cfg/l3/ikev2
IKEv2 Configuration Menu

```
[IKEv2 Menu]
  prop     - IKEv2 Proposal Menu
  tx-time  - Set retransmission timeout for IKEv2 negotiation
  psk      - Preshare Key Menu
  ident    - Certification Service Menu
  cookie   - Enable or Disable cookie notification, used to prevent DoS
  cur      - Display current IKEv2 configuration
```

Table 290 describes the commands used to configure IKEv2.

Table 290. IKEv2 Menu Options (/cfg/l3/ikev2)

Command Syntax and Usage
`prop` Displays the IKEv2 Proposal Menu. To view menu options, see page 358.
`tx-time` *<1-20>* Sets the retransmission timeout, in seconds, for IKEv2 negotiation. The default value is 20 seconds.
`psk` Displays the IKEv2 Preshare Key Menu. To view menu options, see page 358.
`ident` Displays the IKEv2 Identification Menu. To view menu options, see page 359.
`cookie enable|disable` Enables or disables cookie notification. The default value is `disable`.
`cur` Displays the current IKEv2 settings.

/cfg/l3/ikev2/prop

IKEv2 Proposal Configuration Menu

```
[IKEv2 Proposal Menu]
     cipher   - Set encryption algorithm
     auth     - Set the integrity algorithm type
     group    - Set DH group
     cur      - Display current IKEv2 proposal configuration
```

Table 291 describes the commands used to configure an IKEv2 proposal.

Table 291. IKEv2 Proposal Menu Options (/cfg/l3/ikev2/prop)

Command Syntax and Usage
`cipher des|3des|aes` Sets the encryption algorithm. The default value is `3des`.
`auth sha1|md5|none` Sets the authentication algorithm type. The default value is `sha1`.
`group 1|2|5|14|24` Sets the Diffie-Hellman (DH) group. The default group is 2.
`cur` Displays the current IKEv2 proposal settings.

/cfg/l3/ikev2/psk

IKEv2 Preshare Key Configuration Menu

```
[IKEv2 Preshare-key Menu]
     loc-key  - Set local preshare key
     rem-key  - Remote Preshare Key Menu
     cur      - Display current IKEv2 preshare key configuration
```

Table 292 describes the commands used to configure an IKEv2 preshared key.

Table 292. IKEv2 Preshare Key Menu Options (/cfg/l3/ikev2/psk)

Command Syntax and Usage
`loc-key` *<1-256 characters>* Sets the local preshare key. The default value is `ibm123`.
`rem-key` *<1-10>* Displays the Remote ID menu. To view menu options, see page 359.
`cur` Displays the current IKEv2 preshare key settings.

/cfg/l3/ikev2/psk/rem-key <1-10>

IKEv2 Preshare Key Remote ID Configuration Menu

```
[Remote ID 1 Menu]
     addr     - Set remote IPv6 address
     key      - Set remote preshare key
     del      - Delete remote preshare key
     cur      - Display remote preshare key configuration
```

Table 293 describes the commands used to configure an IKEv2 preshared key remote ID.

Table 293. IKEv2 Remote ID Menu Options (/cfg/l3/ikev2/psk/rem-key)

Command Syntax and Usage
`addr` *<IPv6 address>* Sets the remote IPv6 address.
`key` *<1-32 characters>* Sets the remote preshare key. The default value is `ibm123`.
`del` Deletes the remote preshare key.
`cur` Displays the current IKEv2 preshare key remote ID settings.

/cfg/l3/ikev2/ident

IKEv2 Identification Configuration Menu

```
[IKEv2 Identification Menu]
     addr     - Set IPv6 address as identification
     fqdn     - Set fully-qualified domain name as identification
     email    - Set email address as identification
     cur      - Display current IKEv2 identification configuration
```

Table 294 describes the commands used to configure IKEv2 identification.

Table 294. IKEv2 Identification Menu Options (/cfg/l3/ikev2/ident)

Command Syntax and Usage
`addr` *<IPv6 address>* Sets the supplied IPv6 address as identification.
`fqdn` *<fully-qualified domain name>* Sets the fully-qualified domain name (such as “example.com”) as identification.

Table 294. IKEv2 Identification Menu Options (/cfg/l3/ikev2/ident) (continued)

Command Syntax and Usage
`email` *<Email address>* Sets the supplied email address (such as “xyz@example.com”) as identification.
`cur` Displays the current IKEv2 identification settings.

/cfg/l3/ipsec
IPsec Configuration Menu

```
[IPsec Menu]
     txform   - IPSec transform-set Menu
     selector - IPSec traffic-selector Menu
     policy   - IPSec policy Menu
     on       - Globally turn IPsec ON
     off      - Globally turn IPsec OFF
     cur      - Display current IPSec configuration
```

Table 295 describes the commands used to configure IPsec.

Table 295. IPsec Menu Options (/cfg/l3/ipsec)

Command Syntax and Usage
`txform` *<1-10>* Displays the Transform Set Menu. To view menu options, see page 361.
`selector` *<1-10>* Displays the Traffic Selector Menu. To view menu options, see page 362.
`policy` Displays the IPsec Policy Menu. To view menu options, see page 363.
`on` Globally turns on IPsec.
`off` Globally turns off IPsec.
`cur` Displays the current IPsec settings.

/cfg/l3/ipsec/txform

IPsec Transform Set Configuration Menu

```
[Transform_set 1 Menu]
     cipher   - Set ESP encryption algorithm
     integy   - Set ESP integrity algorithm
     auth     - Set AH authentication algorithm
     mode     - Set tunnel/transport mode
     del      - Delete transform
     cur      - Display current IPSec transform setting configuration
```

Table 296 describes the commands used to configure an IPsec transform set.

Table 296. IPsec Transform Set Menu Options (/cfg/l3/ipsec/txform)

Command Syntax and Usage
`cipher esp-des|esp-3des|esp-aes-cbc|esp-null` Sets the ESP encryption algorithm.
`integy esp-sha1|esp-md5|none` Sets the ESP integrity algorithm.
`auth ah-sha1|ah-md5|none` Sets the AH authentication algorithm.
`mode tunnel|txport` Sets tunnel or transport mode. The default is `txport`.
`del` Deletes the transform set.
`cur` Displays the current IPsec Transform Set settings.

/cfg/l3/ipsec/selector

IPsec Traffic Selector Configuration Menu

```
[Traffic_selector 1 Menu]
     action   - Set permit or deny
     proto    - Protocol match Menu
     src      - Set source ip address
     prefix   - Set destination ip address prefix length
     dst      - Set destination ip address
     del      - Delete traffic-selector
     cur      - Display current IPSec selector configuration
```

Table 297 describes the commands used to configure an IPsec traffic selector.

Table 297. IPsec Transform Set Menu Options (/cfg/l3/ipsec/selector)

Command Syntax and Usage
`action permit|deny` Configures the selector to permit or deny traffic.
`proto` Displays the IPsec Protocol Match menu. To view menu options, see page 363.
`src` *<IPv6 address>*`|any` Sets the source IP address.
`prefix` *<1-128>* Sets the destination IPv6 prefix length.
`dst` *<IPv6 address>*`|any` Sets the destination IP address.
`del` Deletes the traffic selector.
`cur` Displays the current IPsec Traffic Selector settings.

/cfg/l3/ipsec/selector/proto

IPsec Protocol Match Configuration Menu

```
[Protocol Menu]
     icmp     - Set icmp for traffic selector
     tcp      - Set tcp for traffic selector
     any      - Set any for traffic
```

Table 298 describes the commands used to configure IPsec protocol matching.

Table 298. IPsec Protocol Match Menu Options (/cfg/l3/ipsec/selector/proto)

Command Syntax and Usage
`icmp` *<ICMP type>* | `any` Sets the ICMP type for the traffic selector.
`tcp` Sets TCP for the traffic selector.
`any` Sets “any” for traffic.

/cfg/l3/ipsec/policy

IPsec Policy Configuration Menu

```
[Policy Menu]
     dynamic  - Dynamic key management policy Menu
     manual   - Manual key management policy Menu
     cur      - Display current IPSec policy configuration
```

Table 299 describes the commands used to configure an IPsec policy.

Table 299. IPsec Policy Menu Options (/cfg/l3/ipsec/policy)

Command Syntax and Usage
`dynamic` *<1-10>* Displays the IPsec Dynamic Policy menu. To view menu options, see page 364.
`manual` *<1-10>* Displays the IPsec Manual Policy menu. To view menu options, see page 365.
`cur` Displays the current IPsec Policy settings.

/cfg/l3/ipsec/policy/dynamic <1-10>

IPsec Dynamic Policy Configuration Menu

```
[Dynamic_policy 1 Menu]
     peer     - Set the remote peer ip address
     selector - Set traffic-selector for IPSec policy
     txform   - Set transform set for IPsec policy
     lifetime - Set IPSec SA lifetime
     pfs      - Configure perfect forward security
     del      - Delete IPsec dynamic policy
     cur      - Display current IPSec dynamic key policy configuration
```

Table 300 describes the commands used to configure an IPsec dynamic policy.

Table 300. IPsec Dynamic Policy Menu Options (/cfg/l3/ipsec/policy/dynamic)

Command Syntax and Usage
`peer` *<IPv6 address>* Sets the remote peer IP address.
`selector` *<1-10>* Sets the traffic selector for the IPsec policy.
`txform` *<1-10>* Sets the transform set for the IPsec policy.
`lifetime` *<120-86400>* Sets the IPsec SA lifetime in seconds. The default value is 86400 seconds.
`pfs enable|disable` Enables or disables perfect forward security.
`del` Deletes the selected dynamic policy configuration.
`cur` Displays the current IPsec dynamic policy settings.

/cfg/l3/ipsec/policy/manual <1-10>

IPsec Manual Policy Configuration Menu

```
[Manual_policy 1 Menu]
     peer     - Set the remote peer ip address
     selector - Set traffic-selector for IPSec policy
     txform   - Set transform set for IPSec policy
     in-ah    - AH inbound session options Menu
     in-esp   - ESP inbound session options Menu
     out-ah   - AH outbound session options Menu
     out-esp  - ESP outbound session options Menu
     del      - Delete IPsec manual policy
     cur      - Display current IPSec manual key policy configuration
```

Table 301 describes the commands used to configure an IPsec manual policy.

Table 301. IPsec Manual Policy Menu Options (/cfg/l3/ipsec/policy/manual)

Command Syntax and Usage
`peer` *<IPv6 address>* Sets the remote peer IP address.
`selector` *<1-10>* Sets the traffic selector for the IPsec policy.
`txform` *<1-10>* Sets the transform set for the IPsec policy.
`in-ah` Displays the Inbound AH Session Options menu. To view menu options, see page 366.
`in-esp` Displays the Inbound ESP Session Options menu. To view menu options, see page 366.
`out-ah` Displays the Outbound AH Session Options menu. To view menu options, see page 367.
`out-esp` Displays the Outbound ESP Session Options menu. To view menu options, see page 368.
`del` Deletes the selected manual policy configuration.
`cur` Displays the current IPsec manual policy settings.

/cfg/l3/ipsec/policy/manual <1-10>/in-ah

IPsec Manual Policy In-AH Configuration Menu

```
[in-ah Menu]
     auth-key - Set inbound AH authenticator key
     spi      - Set inbound AH SPI
     reset    - Reset to factory setting
     cur      - Display current IPSec manual key policy inbound AH
                session configuration
```

Table 302 describes the commands used to configure an IPsec manual policy inbound authentication header (AH).

Table 302. IPsec Manual Policy In-AH Menu Options (/cfg/l3/ipsec/policy/manual/in-ah)

Command Syntax and Usage
`auth-key` *<key code (hexadecimal)>* Sets inbound AH authenticator key.
`spi` *<256-4294967295>* Sets the inbound AH Security Parameter Index (SPI).
`reset` Resets the inbound AH settings to factory settings.
`cur` Displays the current IPsec manual key policy inbound AH session settings.

/cfg/l3/ipsec/policy/manual <1-10>/in-esp

IPsec Manual Policy In-ESP Configuration Menu

```
[in-esp Menu]
     enc-key  - Set inbound ESP cipher key
     auth-key - Set inbound ESP authenticator key
     spi      - Set inbound ESP SPI
     reset    - Reset to factory setting
     cur      - Display current IPSec manual key policy inbound ESP
                session configuration
```

Table 303 describes the commands used to configure an IPsec manual policy inbound Encapsulating Security Payload (ESP) header.

Table 303. IPsec Manual Policy In-ESP Menu Options (/cfg/l3/ipsec/policy/manual/in-esp)

Command Syntax and Usage
`enc-key` *<key code (hexadecimal)>* Sets inbound ESP cipher key.
`auth-key` *<key code (hexadecimal)>* Sets inbound ESP authenticator key.

Table 303. IPsec Manual Policy In-ESP Menu Options (/cfg/l3/ipsec/policy/manual/in-esp) (continued)

Command Syntax and Usage
`spi` *<256-4294967295>* Sets the inbound ESP Security Parameter Index (SPI).
`reset` Resets the inbound ESP settings to factory settings.
`cur` Displays the current IPsec manual key policy inbound ESP session settings.

/cfg/l3/ipsec/policy/manual *<1-10>*/out-ah

IPsec Manual Policy Out-AH Configuration Menu

```
[out-ah Menu]
     auth-key - Set the remote peer ip address
     spi      - Set outbound AH SPI
     reset    - Reset to factory setting
     cur      - Display current IPSec manual key policy outbound AH
                session configuration
```

Table 304 describes the commands used to configure an IPsec manual policy outbound authentication header (AH).

Table 304. IPsec Manual Policy Out-AH Menu Options (/cfg/l3/ipsec/policy/manual/out-ah)

Command Syntax and Usage
`auth-key` *<key code (hexadecimal)>* Sets the remote AH authenticator key.
`spi` *<256-4294967295>* Sets the outbound AH Security Parameter Index (SPI).
`reset` Resets the outbound AH settings to factory settings.
`cur` Displays the current IPsec manual key policy outbound AH session settings.

/cfg/l3/ipsec/policy/manual <1-10>/out-esp

IPsec Manual Policy Out-ESP Configuration Menu

```
[out-esp Menu]
     enc-key  - Set outbound ESP cipher key
     auth-key - Set outbound ESP authenticator key
     spi      - Set outbound ESP SPI
     reset    - Reset to factory setting
     cur      - Display current IPSec manual key policy outbound ESP
                session configuration
```

Table 305 describes the commands used to configure an IPsec manual policy outbound Encapsulating Security Payload (ESP) header.

Table 305. IPsec Manual Policy Out-ESP Menu Options (/cfg/l3/ipsec/policy/manual/out-esp)

Command Syntax and Usage
`enc-key` *<key code (hexadecimal)>* Sets the outbound ESP cipher key.
`auth-key` *<key code (hexadecimal)>* Sets outbound ESP authenticator key.
`spi` *<256-4294967295>* Sets the outbound Security Parameter Index (SPI).
`reset` Resets the outbound ESP settings to factory settings.
`cur` Displays the current IPsec manual key policy outbound ESP session settings.

/cfg/l3/dns
Domain Name System Configuration Menu

```
[Domain Name System Menu]
     prima    - Set IP address of primary DNS server
     secon    - Set IP address of secondary DNS server
     dname    - Set default domain name
     cur      - Display current DNS configuration
```

The Domain Name System (DNS) Menu is 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 306. Domain Name Service Menu Options (/cfg/l3/dns)

Command Syntax and Usage
`prima` *<IPv4 or IPv6 address>* Sets the IPv4 or IPv6 address for your primary DNS server.
`secon` *<IPv4 or IPv6 address>* Sets the IPv4 or IPv6 address for your secondary DNS server. If the primary DNS server fails, the configured secondary is used instead.
`dname` *<dotted DNS notation>*|`none` Sets the default domain name used by the switch. For example: `mycompany.com`
`cur` Displays the current Domain Name System settings.

/cfg/l3/bootp
Bootstrap Protocol Relay Configuration Menu

```
[Bootstrap Protocol Relay Menu]
     server   - Set BOOTP server properties
     bdomain  - Broadcast domain menu
     on       - Globally turn BOOTP relay ON
     off      - Globally turn BOOTP relay OFF
     cur      - Display current BOOTP relay configuration
```

The Bootstrap Protocol (BOOTP) Relay Menu is used to allow hosts to obtain their configurations from a Dynamic Host Configuration Protocol (DHCP) server. The BOOTP configuration enables the switch to forward a client request for an IP address to two DHCP/BOOTP servers with IP addresses that have been configured on the CN4093.

BOOTP relay is turned off by default.

Table 307. Global BOOTP Relay Configuration Options

Command Syntax and Usage
`server <1-4>` Displays the BOOTP Server menu, which allows you to configure an IP address for up to 4 global BOOTP servers. To view menu options, see page 370.
`bdomain <1-10>` Displays the BOOTP Broadcast Domain menu, which allows you to configure BOOTP servers for a specific broadcast domain. To view menu options, see page 371.
`on` Globally turns on BOOTP relay.
`off` Globally turns off BOOTP relay.
`cur` Displays the current BOOTP relay configuration.

/cfg/l3/bootp/server <1-4>
BOOTP Relay Server Configuration

```
[BOOTP Server 2 Menu]
     address  - Set BOOTP server address
     delete   - Delete BOOTP server
```

This menu allows you to configure an IP address for a global BOOTP server.

Table 308. BOOTP Relay Server Configuration Options

Command Syntax and Usage
`address <IPv4 address>` Sets the IP address of the BOOTP server.
`delete` Deletes the selected BOOTP server configuration.

/cfg/l3/bootp/bdomain <*1-10*>

BootP Relay Broadcast Domain Configuration

```
[Broadcast Domain 2 Menu]
     vlan     - VLAN number
     server   - Set IP address of BOOTP server
     enable   - Enable broadcast domain
     disable  - Disable broadcast domain
     delete   - Delete broadcast domain
     cur      - Display current broadcast domain configuration
```

This menu allows you to configure a BOOTP server for a specific broadcast domain, based on its associated VLAN.

Table 309. BOOTP Relay Broadcast Domain Configuration Options

Command Syntax and Usage
`vlan` <*VLAN number*> Configures the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN.
`server` <*1-4*> Displays the BOOTP Server menu, which allows you to configure an IP address for the BOOTP server. To view menu options, see page 370.
`enable` Enables BOOTP Relay for the broadcast domain.
`disable` Disables BOOTP Relay for the broadcast domain. When disabled, BOOTP Relay is performed by one of the global BOOTP servers.
`delete` Deletes the selected broadcast domain configuration.
`cur` Displays the current parameters for the BOOTP Relay Broadcast Domain.

/cfg/l3/vrrp

VRRP Configuration Menu

```
[Virtual Router Redundancy Protocol Menu]
      vr      - VRRP Virtual Router menu
      group   - VRRP Virtual Router Group menu
      if      - VRRP Interface menu
      track   - VRRP Priority Tracking menu
      hotstan - Enable/disable hot-standby processing
      on      - Globally turn VRRP ON
      off     - Globally turn VRRP OFF
      cur     - Display current VRRP configuration
```

Virtual Router Redundancy Protocol (VRRP) support on CN4093s provides redundancy between routers in a LAN. This is accomplished by configuring the same virtual router IP address and ID number on each participating VRRP-capable routing device. One of the virtual routers is then elected as the master, based on a number of priority criteria, and assumes control of the shared virtual router IP address. If the master fails, one of the backup virtual routers will assume routing authority and take control of the virtual router IP address.

By default, VRRP is disabled. IBM Networking OS has extended VRRP to include virtual servers as well, allowing for full active/active redundancy between switches. For more information on VRRP, see the “High Availability” chapter in the *Application Guide*.

Table 310. VRRP Menu Options (/cfg/l3/vrrp)

Command Syntax and Usage
`vr` *<virtual router number (1-128)>* Displays the VRRP Virtual Router Menu. This menu is used for configuring virtual routers on this switch. To view menu options, see page 373.
`group` Displays the VRRP virtual router group menu, used to combine all virtual routers together as one logical entity. Group options must be configured when using two or more switches in a hot-standby failover configuration where only one switch is active at any given time. To view menu options, see page 376.
`if` *<interface number>* Displays the VRRP Virtual Router Interface Menu. To view menu options, see page 378.
`track` Displays the VRRP Tracking Menu. This menu is used for weighting the criteria used when modifying priority levels in the master router election process. To view menu options, see page 379.
`hotstan disable|enable` Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled.
`on` Globally enables VRRP on this switch.

Table 310. VRRP Menu Options (/cfg/l3/vrrp) (continued)

Command Syntax and Usage
`off` Globally disables VRRP on this switch.
`cur` Displays the current VRRP parameters.

/cfg/l3/vrrp/vr <router number>
Virtual Router Configuration Menu

```
[VRRP Virtual Router 1 Menu]
      track   - Priority Tracking Menu
      vrid    - Set virtual router ID
      addr    - Set IP address
      if      - Set interface number
      prio    - Set router priority
      adver   - Set advertisement interval
      preem   - Enable or disable preemption
      ena     - Enable virtual router
      dis     - Disable virtual router
      del     - Delete virtual router
      cur     - Display current VRRP virtual router configuration
```

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 311. VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr)

Command Syntax and Usage
`track` Displays the VRRP Priority Tracking Menu for this virtual router. Tracking is a IBM Networking OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 375.
`vrid` *<virtual router ID (1-255)>* Defines the virtual router ID. This is used in conjunction with `addr` (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same `vrid` and `addr` combination. The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1. All `vrid` values must be unique within the VLAN to which the virtual router's IP interface belongs.

Table 311. VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr) (continued)

Command Syntax and Usage
`addr` *<IP address (such as, 192.4.17.101)>* Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.
`if` *<interface number>* Selects a switch IP interface. If the IP interface has the same IP address as the `addr` option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the `preem` option below is disabled. The default interface is 1.
`prio` *<1-254>* Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used (`/cfg/l3/vrrp/track` or `/cfg/l3/vrrp/vr #/track`), this base priority value can be modified according to a number of performance and operational criteria.
`adver` *<1-255>* Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.
`preem disable|enable` Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.
`ena` Enables this virtual router.
`dis` Disables this virtual router.
`del` Deletes this virtual router from the switch configuration.
`cur` Displays the current configuration information for this virtual router.

/cfg/l3/vrrp/vr <router number>/track

Virtual Router Priority Tracking Configuration Menu

```
[VRRP Virtual Router 1 Priority Tracking Menu]
      vrs     - Enable/disable tracking master virtual routers
      ifs     - Enable/disable tracking other interfaces
      ports   - Enable/disable tracking VLAN switch ports
      cur     - Display current VRRP virtual router configuration
```

This menu is used for modifying the priority system used when electing the master router from a pool of virtual routers. Various tracking criteria can be used to bias the election results. Each time one of the tracking criteria is met, the priority level for the virtual router is increased by an amount defined through the VRRP Tracking Menu (see page 379).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router pre-emption option (see `preem` in Table 311 on page 373) is enabled, this virtual router can assume master routing authority when its priority level rises above that of the current master.

Some tracking criteria (`vrs`, `ifs`, and `ports` below) apply to standard virtual routers, otherwise called “virtual interface routers.” A virtual *server* router is defined as any virtual router whose IP address (`addr`) is the same as any configured virtual server IP address.

Table 312. Virtual Router Priority Tracking Options (/cfg/l3/vrrp/vr #/track)

Command Syntax and Usage
`vrs disable|enable` When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.
`ifs disable|enable` When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
`ports disable|enable` When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
`cur` Displays the current configuration for priority tracking for this virtual router.

/cfg/l3/vrrp/group
Virtual Router Group Configuration Menu

```
[VRRP Virtual Router Group Menu]
      track   - Priority Tracking Menu
      vrid    - Set virtual router ID
      if      - Set interface number
      prio    - Set renter priority
      adver   - Set advertisement interval
      preem   - Enable or disable preemption
      ena     - Enable virtual router
      dis     - Disable virtual router
      del     - Delete virtual router
      cur     - Display current VRRP virtual router configuration
```

The Virtual Router Group menu is used for associating all virtual routers into a single logical virtual router, which forces all virtual routers on the CN4093 to either be master or backup as a group. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Note: This option is required to be configured only when using at least two CN4093s in a hot-standby failover configuration, where only one switch is active at any time.

Table 313. Virtual Router Group Menu Options (/cfg/l3/vrrp/group)

Command Syntax and Usage
`track` Displays the VRRP Priority Tracking Menu for the virtual router group. Tracking is a IBM Networking OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 378.
`vrid` *<virtual router ID (1-255)>* Defines the virtual router ID. The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. All `vrid` values must be unique within the VLAN to which the virtual router's IP interface (see `if` below) belongs. The default virtual router ID is 1.
`if` *<interface number>* Selects a switch IP interface. The default switch IP interface number is 1.

Table 313. Virtual Router Group Menu Options (/cfg/l3/vrrp/group) (continued)

Command Syntax and Usage
`prio <1-254>` Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. Each virtual router group is treated as one entity regardless of how many virtual routers are in the group. When the switch tracks the virtual router group, it measures the resources contained in the group (such as interfaces, VLAN ports, real servers). The priority is updated as a group. Every virtual router in the group has the same priority. The *owner* parameter does not apply to the virtual router group. The group itself cannot be an owner and therefore the priority is 1-254.
`adver <1-255>` Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.
`preem disable|enable` Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.
`ena` Enables the virtual router group.
`dis` Disables the virtual router group.
`del` Deletes the virtual router group from the switch configuration.
`cur` Displays the current configuration information for the virtual router group.

/cfg/l3/vrrp/group/track

Virtual Router Group Priority Tracking Configuration Menu

```
[Virtual Router Group Priority Tracking Menu]
      ifs     - Enable/disable tracking other interfaces
      ports   - Enable/disable tracking VLAN switch ports
      cur     - Display current VRRP Group Tracking configuration
```

Note: If *Virtual Router Group Tracking* is enabled, then the tracking option will be available only under *group* option. The tracking setting for the other individual virtual routers will be ignored.

Table 314. Virtual Router Group Priority Tracking Menu (/cfg/l3/vr/group/track)

Command Syntax and Usage
`ifs disable|enable` When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
`ports disable|enable` When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.
`cur` Displays the current configuration for priority tracking for this virtual router.

/cfg/l3/vrrp/if *<interface number>*

VRRP Interface Configuration Menu

Note: The *interface-number* represents the IP interface on which authentication parameters must be configured.

```
[VRRP Interface 1 Menu]
      auth    - Set authentication types
      passw   - Set plain-text password
      del     - Delete interface
      cur     - Display current VRRP interface configuration
```

This menu is used for configuring VRRP authentication parameters for the IP interfaces used with the virtual routers.

Table 315. VRRP Interface Menu Options (/cfg/l3/vrrp/if)

Command Syntax and Usage
`auth none|password` Defines the type of authentication that will be used: `none` (no authentication), or `password` (password authentication).
`passw` *<password>* Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see `auth` above).
`del` Clears the authentication configuration parameters for this IP interface. The IP interface itself is not deleted.
`cur` Displays the current configuration for this IP interface's authentication parameters.

/cfg/l3/vrrp/track
VRRP Tracking Configuration Menu

```
[VRRP Tracking Menu]
      vrs     - Set priority increment for virtual router tracking
      ifs     - Set priority increment for IP interface tracking
      ports   - Set priority increment for VLAN switch port tracking
      cur     - Display current VRRP Priority Tracking configuration
```

This menu is used for setting weights for the various criteria used to modify priority levels during the master router election process. Each time one of the tracking criteria is met (see "VRRP Virtual Router Priority Tracking Menu" on page 375), the priority level for the virtual router is increased by an amount defined through this menu.

Table 316. VRRP Tracking Menu Options (/cfg/l3/vrrp/track)

Command Syntax and Usage
`vrs` *<0-254>* Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.
`ifs` *<0-254>* Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.

Table 316. VRRP Tracking Menu Options (/cfg/l3/vrrp/track) (continued)

Command Syntax and Usage
`ports` *<0-254>* Defines the priority increment value (0 through 254) for active ports on the virtual router's VLAN. The default value is 2.
`cur` Displays the current configuration of priority tracking increment values.

Note: These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Menu (see page 375) are enabled.

/cfg/l3/gw6 *<gateway number>*
IPv6 Default Gateway Configuration Menu

```
[Default IP6 gateway 1 Menu]
     addr     - Set IP address
     ena      - Enable default gateway
     dis      - Disable default gateway
     del      - Delete default gateway
     cur      - Display current default gateway configuration
```

The switch supports IPv6 default gateways:

- Gateway 1 is used for data traffic.
- Gateways 3 and 4 are reserved for management.

The following table describes the IPv6 default gateway configuration options.

Table 317. IPv6 Default Gateway Menu Options (/cfg/l3/gw6)

Command Syntax and Usage
`addr` *<IPv6 address, such as 3001:0:0:0:0:0:abcd:12>* Configures the IPv6 address of the default gateway, in hexadecimal format with colons.
`ena` Enables the default gateway.
`dis` Disables the default gateway.
`del` Deletes the default gateway.
`cur` Displays current IPv6 default gateway settings.

/cfg/l3/route6

IPv6 Static Route Configuration Menu

```
[IP6 Static Route Menu]
     add      - Add static route
     rem      - Remove static route
     clear    - Clear static routes
     cur      - Display current IP6 static route configuration
```

The following table describes the IPv6 static route configuration options.

Table 318. IP6 Static Route Menu Options (/cfg/l3/route6)

Command Syntax and Usage
`add` *<IPv6 address, such as 3001:0:0:0:0:0:abcd:12> <Prefix length> <gateway address>* [*<interface number>*] Adds an IPv6 static route.
`rem` *<IPv6 address, such as 3001:0:0:0:0:0:abcd:12> <Prefix length>* [*<interface number>*] Removes the IPv6 static route.
`clear` Clears IPv6 static routes. You are prompted to select the routes to clear, based on the following criteria: – `dest`: Destination IPv6 address of the route – `gw`: Default gateway address used by the route – `if`: Interface used by the route – `all`: All IPv6 static routes
`cur` Displays the current IPv6 static route configuration.

/cfg/l3/nbrcache

IPv6 Neighbor Discovery Cache Configuration Menu

```
[Static NBR Cache Menu]
     add      - Add a static NBR Cache entry
     del      - Delete a static NBR Cache entry
     clear    - Clear static neighbor cache table
     cur      - Display current static NBR Cache configuration
```

The following table describes the IPv6 Neighbor Discovery cache configuration options.

Table 319. Static NBR Cache Menu Options (/cfg/l3/nbrcache)

Command Syntax and Usage
`add` *<IPv6 address, such as 3001:0:0:0:0:0:abcd:12> <MAC address, such as 00:60:af:00:02:30> <VLAN number> <port number or alias>* Adds a static entry to the Neighbor Discovery cache table. You are prompted for the following information: – IP address – MAC address – VLAN number – Port
`del` *<IPv6 address, such as 3001:0:0:0:0:0:abcd:12>* Deletes the selected entry from the Neighbor Discovery cache table.
`clear` Clears static entries in the Neighbor Discovery cache table. You are prompted to select the entries to clear, based on the following criteria: – `IF`: Entries associated with the selected interface – `VLAN`: Entries associated with the selected VLAN – `Port`: Entries associated with the selected port – `All`: All IPv6 Neighbor cache entries.
`cur` Displays the current configuration of the Neighbor Discovery static cache table.

/cfg/l3/ip6pmtu

IPv6 Path MTU Configuration

```
[IP6 Path MTU Menu]
     timeout  - Set timeout duration of PMTU cache in minutes
     clear    - Clear IP6 Path MTU stats
     cur      - Display current PMTU 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 320. IPv6 Path MTU Options

Command Syntax and Usage
`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.
`clear` Clears all entries in the Path MTU cache.
`cur` Displays the current Path MTU configuration.

/cfg/l3/ospf3

Open Shortest Path First Version 3 Configuration Menu

```
[Open Shortest Path First v3 Menu]
     aindex   - OSPFv3 Area (index) Menu
     range    - OSPFv3 Summary Range Menu
     summpref - OSPFv3 AS-External Range Menu
     if       - OSPFv3 Interface Menu
     virt     - OSPFv3 Virtual Links Menu
     host     - OSPFv3 Host Entry Menu
     rdstcfg  - OSPFv3 Route Redistribute Entry Menu
     redist   - OSPFv3 Route Redistribution Menu
     abrtype  - Set the alternative ABR type
     lsdb     - Set the LSDB limit for external LSA
     exoverfl - Set exit overflow interval in seconds
     refbw    - Set reference bandwidth for dflt intf metric calc
     spfdelay - Set delay between topology change and SPF calc
     spfhold  - Set hold time between two consecutive SPF calc
     rtrid    - Set a fixed router ID
     nasbrdfr - Enable/disable set P-bit by an NSSA internal ASBR
     on       - Globally turn OSPFv3 ON
     off      - Globally turn OSPFv3 OFF
     cur      - Display current OSPFv3 configuration
```

Table 321. OSPFv3 Configuration Menu (/cfg/l3/ospf3)

Command Syntax and Usage
`aindex` *<area index (0-2)>* Displays the area index menu. This area index does not represent the actual OSPFv3 area number. See page 386 to view menu options.
`range` *<1-16>* Displays summary routes menu for up to 16 IP addresses. See page 387 to view menu options.
`summpref` *<1-16>* Displays the OSPFv3 summary prefix configuration menu. See page 389 to view menu options.
`if` *<interface number>* Displays the OSPFv3 interface configuration menu. See page 390 to view menu options.
`virt` *<virtual link (1-3)>* Displays the Virtual Links menu used to configure OSPFv3 for a Virtual Link. See page 394 to view menu options.
`host` *<1-128>* Displays the menu for configuring OSPFv3 for the host routes. Up to 128 host routes can be configured. Host routes are used for advertising network device IP addresses to external networks to perform server load balancing within OSPF. It also makes Area Border Route (ABR) load sharing and ABR failover possible. See page 395 to view menu options.

Table 321. OSPFv3 Configuration Menu (/cfg/l3/ospf3) (continued)

Command Syntax and Usage
`rdstcfg` *<1-128>* Displays the OSPF route redistribution entry menu. See page 396 to view menu options.
`redist connected|static` Displays route redistribution menu. See page 397 to view menu options.
`abrtype {standard|cisco|ibm}` Configures the Area Border Router (ABR) type, as follows: – Standard – Cisco – IBM The default setting is `standard`.
`lsdb` *<LSDB limit (0-2147483647)>*`|none` Sets the link state database limit.
`exoverfl` *<0-4294967295>* Configures the number of seconds that a router takes to exit Overflow State. The default value is 0 (zero).
`refbw` *<0-4294967295>* Configures the reference bandwidth, in kilobits per second, used to calculate the default interface metric. The default value is 100,000.
`spfdelay` *<0-65535>* Configures the number of seconds that SPF calculation is delayed after a topology change message is received. The default value is 5.
`spfhold` *<0-65535>* Configures the number of seconds between SPF calculations. The default value is 10.
`rtrid` *<IP address>* Defines the router ID.
`nasbrdfr e|d` Enables or disables setting of the P-bit in the default Type 7 LSA generated by an NSSA internal ASBR. The default setting is `disabled`.
`on` Enables OSPFv3 on the switch.
`off` Disables OSPFv3 on the switch.
`cur` Displays the current OSPF configuration settings.

/cfg/l3/ospf3/aindex <*area index*>

Area Index Configuration Menu

```
[OSPFv3 Area (index) 1 Menu]
 areaid   - Set area ID
 type     - Set area type
 metric   - Set metric for the default route into stub/NSSA area
 mettype  - Set default metric for stub/NSSA area
 stb      - Set stability interval for the NSSA area
 trnsrole - Set translation role for the NSSA area
 nosumm   - Enable/disable prevent sending summ LSA into stub/NSSA area
 enable   - Enable area
 disable  - Disable area
 delete   - Delete area
 cur      - Display current OSPF area configuration
```

Table 322. OSPFv3 Area Index Configuration Options (/cfg/l3/ospf3/aindex)

Command Syntax and Usage
areaid <*IP address (such as, 192.4.17.101)*> Defines the IP address of the OSPFv3 area index.
type transit|stub|nssa Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. **Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. **NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.
metric <*metric value (1-16777215)*> Configures the cost for the default summary route in a stub area or NSSA.
mettype <*1-3*> Configures the default metric type applied to the route. This command applies only to area type of Stub/NSSA.
stb <*1-255*> Configures the stability interval for an NSSA, in seconds. When the interval expires, an elected translator determines that its services are no longer required. The default value is 40.

Table 322. OSPFv3 Area Index Configuration Options (/cfg/l3/ospf3/aindex) (continued)

Command Syntax and Usage
`trnsrole always|candidate` Configures the translation role for an NSSA area, as follows: – `always`: Type 7 LSAs are always translated into Type 5 LSAs. – `candidate`: An NSSA border router participates in the translator election process. The default setting is `candidate`.
`nosumm e|d` Enables or disables the no-summary option. When enabled, the area-border router neither originates nor propagates Inter-Area-Prefix LSAs into stub/NSSA areas. Instead it generates a default Inter-Area-Prefix LSA. The default setting is `disabled`.
`enable` Enables the OSPFv3 area.
`disable` Disables the OSPFv3 area.
`delete` Deletes the OSPFv3 area.
`cur` Displays the current OSPFv3 area configuration.

/cfg/l3/ospf3/range *<range number>*

OSPFv3 Summary Range Configuration Menu

```
[OSPFv3 Summary Range 1  Menu]
     addr     - Set IPv6 address
     preflen  - Set IPv6 prefix length
     aindex   - Set area index
     lsatype  - Set LSA type for aggregation
     tag      - Set route tag
     hide     - Enable/disable hide range
     enable   - Enable range
     disable  - Disable range
     delete   - Delete range
     cur      - Display current OSPFv3 summary range configuration
```

Table 323. OSPFv3 Summary Range Configuration Options (/cfg/l3/ospf3/range)

Command Syntax and Usage
`addr` *<IPv6 address>* Configures the base IPv6 address for the range.
`preflen` *<IPv6 prefix length (1-128)>* Configures the subnet IPv6 prefix length. The default value is 0 (zero).

Table 323. OSPFv3 Summary Range Configuration Options (/cfg/l3/ospf3/range)

Command Syntax and Usage
`aindex` *<area index (0-2)>* Configures the area index used by the switch.
`lsatype summary|Type7` Configures the LSA type, as follows: – Summary LSA – Type7 LSA
`tag` *<0-4294967295>* Configures the route tag.
`hide disable|enable` Hides the OSPFv3 summary range.
`enable` Enables the OSPFv3 summary range.
`disable` Disables the OSPFv3 summary range.
`delete` Deletes the OSPFv3 summary range.
`cur` Displays the current OSPFv3 summary range configuration.

/cfg/l3/ospf3/summpref <*range number*>

OSPFv3 AS-External Range Configuration Menu

```
[OSPFv3 AS-External Range 1  Menu]
     addr     - Set IPv6 address
     preflen  - Set IPv6 prefix length
     aindex   - Set area index
     aggreff  - Set aggregation effect
     transl   - Enable/disable set P-bit in the generated LSA
     enable   - Enable range
     disable  - Disable range
     delete   - Delete range
     cur      - Display current OSPFv3 AS-External range configuration
```

Table 324. OSPFv3 AS External Range Configuration Options (/cfg/l3/ospf3/range)

Command Syntax and Usage
addr <*IPv6 address*> Configures the base IPv6 address for the range.
preflen <*IPv6 prefix length (1-128)*> Configures the subnet IPv6 prefix length. The default value is 0 (zero).
aindex <*area index (0-2)*> Configures the area index used by the switch.
aggreff allowAll|denyAll|advertise|not-advertise Configures the aggregation effect, as follows: – allowAll: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. Aggregated Type-7 LSAs are generated in all the attached NSSAs for the range. – denyAll: Type-5 and Type-7 LSAs are not generated. – advertise: If the area ID is 0.0.0.0, aggregated Type-5 LSAs are generated. For other area IDs, aggregated Type-7 LSAs are generated in the NSSA area. – not-advertise: If the area ID is 0.0.0.0, Type-5 LSAs are not generated, while all NSSA LSAs within the range are cleared and aggregated Type-7 LSAs are generated for all NSSAs. For other area IDs, aggregated Type-7 LSAs are not generated in the NSSA area.
transl e|d When enabled, the P-bit is set in the generated Type-7 LSA. When disabled, the P-bit is cleared. The default setting is disabled.
enable Enables the OSPFv3 AS-external range.
disable Disables the OSPFv3 AS-external range.

Table 324. OSPFv3 AS External Range Configuration Options (/cfg/l3/ospf3/range)

Command Syntax and Usage
`delete` Deletes the OSPFv3 AS-external range.
`cur` Displays the current OSPFv3 AS-external range.

/cfg/l3/ospf3/if <*interface number*>
OSPFv3 Interface Configuration Menu

```
[OSPFv3 Interface 1  Menu]
     aindex   - Set area index
     ipsec    - Set ipsec on the interface
     instance - Set instance id
     prio     - Set interface router priority
     cost     - Set interface cost
     hello    - Set hello interval in seconds
     dead     - Set dead interval in seconds
     transm   - Set transmit delay in seconds
     retra    - Set retransmit interval in seconds
     passive  - Enable/disable passive interface
     enable   - Enable interface
     disable  - Disable interface
     delete   - Delete interface
     cur      - Display current OSPFv3 interface configuration
```

Table 325. OSPFv3 Interface Configuration Options (/cfg/l3/ospf3/if)

Command Syntax and Usage
`aindex` <*area index (0-2)*> Configures the OSPFv3 area index.
`ipsec` Displays the OSPFv3 over IPsec configuration menu. See page 391 to view menu options.
`instance` <*0-255*> Configures the instance ID for the interface.
`prio` <*priority value (0-255)*> Configures the priority value for the switch's OSPFv3 interface. A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR).
`cost` <*1-65535*> Configures the metric value for sending a packet on the interface.
`hello` <*1-65535*> Configures the indicated interval, in seconds, between the `hello` packets, that the router sends on the interface.

Table 325. OSPFv3 Interface Configuration Options (/cfg/l3/ospf3/if) (continued)

Command Syntax and Usage
`dead` *<1-65535>* Configures the time period, in seconds, for which the router waits for `hello` packet from the neighbor before declaring this neighbor down.
`transm` *<1-1800>* Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.
`retra` *<1-1800>* Configures the interval in seconds, between LSA retransmissions for adjacencies belonging to interface.
`passive enable|disable` Enables or disables the `passive` setting on the interface. On a passive interface, OSPFv3 protocol packets are suppressed.
`enable` Enables the OSPFv3 interface.
`disable` Disables the OSPFv3 interface.
`delete` Deletes the OSPFv3 interface.
`cur` Displays the current settings for OSPFv3 interface.

/cfg/l3/ospf3/if *<interface number>*/ipsec

OSPFv3 IPsec Configuration Menu

```
[OSPFv3 Interface 1 IPSec Menu]
     ah       - Set AH protocol
     esp      - Set ESP protocol
```

The following menus enable you to configure IPsec on OSPFv3.

Table 326. OSPFv3 IPsec Configuration Options (/cfg/l3/ospf3/if/ipsec)

Command Syntax and Usage
`ah` Displays the Authentication Header (AH) configuration menu. To view menu options, see page 392.
`esp` Displays the Encapsulating Security Payload (ESP) configuration menu. To view menu options, see page 393.

/cfg/l3/ospf3/if <*interface number*>/ipsec/ah

OSPFv3 IPsec Authentication Header Configuration Menu

```
[Set AH protocol]
     auth     - Select the authentication algorithm
     authkey  - Set the authentication key
     spi      - Set the security parameter index
     enable   - Enable AH
     disable  - Disable AH
     reset    - Reset AH configuration
     cur      - Display current AH settings
```

The following menus enable you to configure an IPsec Authentication Header on OSPFv3.

Table 327. OSPFv3 IPsec AH Configuration Options (/cfg/l3/ospf3/if/ipsec/ah)

Command Syntax and Usage
`auth sha1 | md5 | none` Sets the authentication algorithm.
`authkey` *<Hexadecimal string (MD5 key - 32 chars|SHA1 key - 40 chars)>* Configures the authentication key password.
`spi` *<256-4294967295>* Sets the IPsec in AH Security Parameter Index (SPI).
`enable` Enables the authentication header.
`disable` Disables the authentication header.
`reset` Resets the AH settings to factory settings.
`current` Displays the current AH configuration.

/cfg/l3/ospf3/if <*interface number*>/ipsec/esp

OSPFv3 over IPsec Configuration Menu

```
[OSPFv3 Interface 1 ESP Menu]
     auth     - Select the authentication algorithm
     authkey  - Set the authentication key
     encrypt  - Select the encryption algorithm
     encrykey - Set the encryption key
     spi      - Set the security parameter index
     enable   - Enable ESP
     disable  - Disable ESP
     reset    - Reset ESP configuration
     cur      - Display current ESP settings
```

The following menus enable you to configure an IPsec Encapsulating Security Payload on OSPFv3.

Table 328. OSPFv3 IPsec ESP Configuration Options (/cfg/l3/ospf3/if/ipsec/esp)

Command Syntax and Usage
`auth sha1 | md5 | none` Sets the authentication algorithm.
`authkey` *<Hexadecimal string (MD5 - 32 chars|SHA1 - 40 chars)>* Configures the authentication key password.
`encrypt des | 3des | aes | null` Sets the encryption algorithm.
`encrykey` *<Hexadecimal string (3DES - 32 chars|AES - 40 chars|DES - 16 chars)>* Sets the encryption key.
`spi` *<256-4294967295>* Sets the IPsec in AH Security Parameter Index (SPI).
`enable` Enables the encapsulating security payload.
`disable` Disables the encapsulating security payload.
`reset` Resets the ESP settings to factory settings.
`current` Displays the current ESP configuration.

/cfg/l3/ospf3/virt <*link number*>

OSPFv3 Virtual Link Configuration Menu

```
[OSPFv3 Virtual Link 1  Menu]
     aindex   - Set area index
     hello    - Set hello interval in seconds
     dead     - Set dead interval in seconds
     trans    - Set transit delay in seconds
     retra    - Set retransmit interval in seconds
     nbr      - Set router ID of virtual neighbor
     enable   - Enable interface
     disable  - Disable interface
     delete   - Delete interface
     cur      - Display current OSPFv3 interface configuration
```

Table 329. OSPFv3 Virtual Link Configuration Options (/cfg/l3/ospf3/virt)

Command Syntax and Usage
aindex <*area index (0-2)*> Configures the OSPFv3 area index.
hello <*1-65535*> Configures the indicated interval, in seconds, between the hello packets, that the router sends on the interface.
dead <*1-65535*> Configures the time period, in seconds, for which the router waits for hello packet from the neighbor before declaring this neighbor down.
trans <*1-1800*> Configures the estimated time, in seconds, taken to transmit LS update packet over this interface.
retra <*1-1800*> Configures the interval, in seconds, between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. The default value is five seconds.
nbr <*NBR router ID (IP address)*> Configures the router ID of the virtual neighbor. The default setting is 0.0.0.0
enable Enables OSPFv3 virtual link.
disable Disables the OSPFv3 virtual link.
delete Deletes the OSPFv3 virtual link.
cur Displays the current OSPFv3 virtual link settings.

/cfg/l3/ospf3/host <*host number*>

OSPFv3 Host Entry Configuration Menu

```
[OSPF Host Entry 1 Menu]
      addr    - Set host entry IP address
      aindex  - Set area index
      cost    - Set cost of this host entry
      enable  - Enable host entry
      disable - Disable host entry
      delete  - Delete host entry
      cur     - Display current OSPF host entry configuration
```

Table 330. OSPFv3 Host Entry Configuration Options (/cfg/l3/ospf3/host)

Command Syntax and Usage
addr <*IPv6 address*> Configures the base IPv6 address for the host entry.
aindex <*area index (0-2)*> Configures the area index of the host.
cost <*1-65535*> Configures the cost value of the host.
enable Enables OSPF host entry.
disable Disables OSPF host entry.
delete Deletes OSPF host entry.
cur Displays the current OSPF host entries.

/cfg/l3/ospf3/rdstcfg <1-128>

OSPFv3 Redist Entry Configuration Menu

```
[OSPFv3 Redist Entry 1 Menu]
     addr     - Set redist entry IPv6 address
     preflen  - Set IPv6 prefix length
     metric   - Set metric to be applied to the route
     mettype  - Set metric type
     tag      - Set route tag
     enable   - Enable redist entry
     disable  - Disable redist entry
     delete   - Delete redist entry
     cur      - Display current OSPF redist entry configuration
```

Table 331. OSPFv3 Redist Entry Configuration Options (/cfg/l3/ospf3/rdstcfg)

Command Syntax and Usage
addr *<IPv6 address>* Configures the base IPv6 address for the redistribution entry.
preflen *<IPv6 prefix length (1-128)>* Configures the subnet IPv6 prefix length. The default value is 64.
metric *<1-16777215>* Configures the route metric value applied to the route before it is advertised into the OSPFv3 domain.
mettype asExttype1|asExttype2 Configures the metric type applied to the route before it is advertised into the OSPFv3 domain.
tag *<0-4294967295>*|unset Configures the route tag. To clear the route tag, enter unset.
enable Enables the OSPFv3 redistribution entry.
disable Disables the OSPFv3 redistribution entry.
delete Deletes the OSPFv3 redistribution entry.
cur Displays the current OSPFv3 redistribution configuration entries.

/cfg/l3/ospf3/redist connected|static

OSPFv3 Redistribute Configuration Menu

```
[OSPF Redistribute Static  Menu]
     export   - Export all routes of this protocol
     cur      - Display current redistribution setting
```

Table 332. OSPFv3 Redistribute Configuration Options (/cfg/l3/ospf3/redist)

Command Syntax and Usage
export [<*metric value (1-16777215)*>|none] [<*metric type (1-2)*>] [<*tag (0-4294967295)*>|unset] Exports the routes of this protocol as external OSPFv3 AS-external LSAs in which the metric, metric type, and route tag are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none. To clear the route tag, enter unset.
cur Displays the current OSPFv3 route redistribution settings.

/cfg/l3/ndprefix

IPv6 Neighbor Discovery Prefix Configuration

```
[IP6 Neighbor Discovery Prefix Menu]
     profile  - Profile of ND Prefix
     add      - Add Neighbour Discovery Prefix
     rem      - Remove Neighbour Discovery Prefix
     clear    - Clear Neighbour Discovery Prefix
     cur      - Display current Neighbour 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 333. IPv6 Neighbor Discovery Prefix Options

Command Syntax and Usage
`profile` *<1-127>* Displays the Neighbor Discovery Profile menu. You can configure up to 127 profiles. You must attach a profile to each Neighbor Discovery prefix.
`add` {*<IPv6 prefix> <prefix length> <interface number> <profile index>*} Adds a Neighbor Discovery prefix to an interface. **Note**: A profile index of 0 (zero) adds the default profile, as follows: – Prefix Advertisement: enabled – Valid Lifetime: 2592000 – Valid Lifetime Fixed Flag: enabled – Preferred Lifetime: 604800 – Preferred Lifetime Fixed Flag: enabled – On-link Flag: enabled – Autonomous Flag: enabled
`rem` {*<IPv6 prefix> <prefix length>*} Removes a Neighbor Discovery prefix.
`clear` *<interface number>*|`all` Clears the selected Neighbor Discovery prefixes. If you include an interface number, all ND prefixes for that interface are cleared.
`cur` Displays current Neighbor Discovery prefix parameters.

/cfg/l3/ndprefix/profile <*1-127*>

IPv6 Neighbor Discovery Profile Configuration

```
[IP6 Neighbor Discovery Profile 1 Menu]
     valft    - Set Prefix Valid lifetime
     valftfix - Set Prefix Valid lifetime FIXED Flag
     prlft    - Set Prefix Preferred lifetime
     prlftfix - Set Prefix Preferred lifetime FIXED Flag
     onlink   - Set Prefix on-link Flag
     autoflag - Set Prefix Autonomous Flag
     ena      - Enable Prefix advertisement
     dis      - Disable Prefix advertisement
     del      - Delete profile
     cur      - Display current Neighbor Discovery Prefix configuration
```

The following table describes the Neighbor Discovery Profile configuration options.Information in the ND profile can be used to supplement information included in an ND prefix.

Table 334. IPv6 Neighbor Discovery Profile Options

Command Syntax and Usage
`valft` <*0-4294967295*> Configures the Valid 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. Enter the maximum value to configure a Valid Lifetime of infinity. The default value is 2592000.
`valftfix enable|disable` Enables of disables the Valid Lifetime fixed flag. When enabled, the Valid Lifetime value represents a fixed time that stays the same in consecutive advertisements. When disabled, the Valid Lifetime value represents a time that decrements in real time, that is, one that will result in a value of zero at a specified time in the future. The default setting is `enabled`.
`prlft` <*0-4294967295*> Configures the Preferred Lifetime of the prefix, in seconds. 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. Enter the maximum value to configure a Preferred Lifetime value of infinity. The default value is 604800. **Note**: The Preferred Lifetime value must not exceed the Valid Lifetime value.

Table 334. IPv6 Neighbor Discovery Profile Options

Command Syntax and Usage
`prlftfix enable|disable` Enables or disables the Preferred Lifetime fixed flag. When enabled, the Preferred Lifetime value represents a fixed time that stays the same in consecutive advertisements. When disabled, the Preferred Lifetime value represents a time that decrements in real time, that is, one that will result in a value of zero at a specified time in the future. The default setting is `enabled`.
`onlink enable|disable` Enables or disables the on-link flag. When enabled, 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`.
`autoflag enable|disable` Enables or disables the autonomous flag. When enabled, indicates that the prefix can be used for stateless address configuration. The default setting is `enabled`.
`ena` Enables the selected profile.
`dis` Disables the selected profile
`del` Delete the selected Neighbor Discovery profile.
`cur` Displays the current Neighbor Discovery profile parameters.

/cfg/l3/ppt

IPv6 Prefix Policy Table Configuration

```
[Prefix Policy Table Menu]
     add      - Add prefix Policy
     rem      - Remove prefix policy
     cur      - Display prefix policy table
```

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

Table 335. IPv6 Prefix Policy Table Options

Command Syntax and Usage
`add` *<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.
`rem` *<IPv6 prefix> <prefix length> <precedence (0-100)> <label (0-100)>* Removes a prefix policy table entry.
`cur` Displays the current Prefix Policy Table configuration.

/cfg/l3/loopif <*interface number (1-5)*>
IP Loopback Interface Configuration Menu

```
[IP Loopback Interface 2 Menu]
     addr     - Set IP address
     mask     - Set subnet mask
     ena      - Enable IP interface
     dis      - Disable IP interface
     del      - Delete IP interface
     cur      - Display current interface configuration
```

An IP loopback interface is not connected to any physical port. A loopback interface is always accessible over the network.

Table 336. IP Loopback Interface Menu Options (/cfg/l3/loopif)

Command Syntax and Usage
addr <*IP address*> Defines the loopback interface IP address.
mask <*subnet mask*> Defines the loopback interface subnet mask.
ena Enables the loopback interface.
dis Disables the loopback interface.
del Deletes the selected loopback interface.
cur Displays the current IP loopback interface parameters.

/cfg/l3/flooding
Flooding Configuration Menu

```
[flooding Menu]
     vlan     - VLAN Flooding Menu
     cur      - Display current Flooding configuration
```

Table 337. Flooding Menu Options (/cfg/l3/flooding)

Command Syntax and Usage
`vlan` *<VLAN number>* Displays the flooding configuration menu for the VLAN. See page 403 to view menu options.
`cur` Displays the current flooding parameters.

/cfg/l3/flooding/vlan *<VLAN number>*
Flooding VLAN Configuration Menu

```
[VLAN 1 Flooding Menu]
     flood    - Flood unregistered IPMC
     cpu      - Send unregistered IPMC to CPU
     optflood - Enable/disable optimized flooding
     cur      - Display current Flooding configuration for this vlan
```

Table 338. Flooding VLAN Menu Options (/cfg/l3/flooding/vlan)

Command Syntax and Usage
`flood enable|disable` 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.
`cpu enable|disable` 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.

Table 338. Flooding VLAN Menu Options (/cfg/l3/flooding/vlan) (continued)

Command Syntax and Usage
`optflood enable|disable` Enables or disables optimized flooding. When enabled, optimized flooding avoids packet loss during the learning period. The default setting is `disabled`.
`cur` Displays the current flooding parameters for the selected VLAN.

/cfg/cee
Converged Enhanced Ethernet Configuration

```
[CEE Configuration Menu]
     global   - Global CEE Configuration Menu
     port     - Port CEE Configuration Menu
     iscsi    - Globally turn ISCSI TLV advertisement ON/OFF
     on       - Globally turn CEE Features ON
     off      - Globally turn CEE Features OFF
     cur      - Display current CEE configuration
```

Table 339 describes the Converged Enhanced Ethernet (CEE) configuration menu options.

Table 339. CEE Configuration Options (/cfg/cee)

Command Syntax and Usage
`global` Displays the CEE Global Configuration menu. To view menu options, see page 405.
`port` Displays the CEE Port Configuration menu. To view menu options, see page 408.
`iscsi e|d` Enables or disables ISCSI TLV advertisements.
`on` Globally turns CEE on.
`off` Globally turns CEE off.
`cur` Displays the current CEE parameters.

/cfg/cee/global
CEE Global Configuration

```
[Global CEE Configuration Menu]
     ets      - Enhanced Transmission Selection Menu
     pfc      - Priority Flow Control Menu
     cur      - Display current CEE configuration
```

Table 340 describes the global CEE configuration options.

Table 340. CEE Global Options (/cfg/cee/global)

Command Syntax and Usage
ets Displays the Enhanced Transmission Selection menu. To view menu options, see page 405.
pfc Displays the Priority Flow Control menu. To view menu options, see page 406.
cur Displays the current global CEE parameters.

/cfg/cee/global/ets
ETS Global Configuration

```
[Global Enhanced Transmission Selection Menu]
     pg       - Priority Group Menu
     cur      - Displays current ETS configuration
```

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

Table 341 describes the global ETS configuration options.

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

Table 341. CEE Global ETS Options (/cfg/cee/global/ets)

Command Syntax and Usage
pg *<0-7, 15>* Displays the Enhanced Transmission Selection menu for the selected Priority Group. To view menu options, see page 406.
cur Displays the current global CEE parameters.

/cfg/cee/global/ets/pg <0-7, 15>

ETS Global Priority Group Configuration

```
[PGID 1 Menu]
     create   - Create Priority Group
     bw       - Set bandwidth percentage for the Priority Group
     prio     - Assign one or more 802.1p priorities to Priority Group
     desc     - Set description for the Priority Group
     cur      - Display current Priority Group configuration
```

An ETS Priority Group can be assigned one or more 802.1p priority values. Switch bandwidth is allocated by percentage to each Priority Group.

Note: The `create` and `bw` options are not available for Priority Group 15.

Table 342 describes the global ETS Priority Group configuration options.

Table 342. Global ETS Priority Group Options (/cfg/cee/global/ets/pg)

Command Syntax and Usage
`create` {*<bandwidth percentage (0, 10-100)>*} *<802.1p value (0-7)>* 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.
`bw` *<bandwidth percentage (0, 10-100)>* Configures the link bandwidth allocation for the Priority Group, as a percentage from 10% to 100%. Enter 0 (zero) to disable bandwidth allocation to the Priority Group.
`prio` *<0-7>* Adds one or more 802.1p priority values to the Priority Group. Enter one value per line, null to end.
`desc` *<1-31 characters>* Enter text that describes this Priority Group.
`cur` Displays the current ETS global Priority Group parameters.

/cfg/cee/global/pfc

Priority Flow Control Global Configuration

```
[Global Priority Flow Control Menu]
     pri      - 802.1p Priority PFC Menu
     on       - Globally turn PFC ON
     off      - Globally turn PFC OFF
     cur      - Display current PFC 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.

Priority-based Flow Control global configuration configure all ports with one command. The difference between ETS and PFC global configuration is that the ETS commands are applied in running as global commands, whereas the PFC commands are applied on a per-port basis even though they are configured from the global menu.

Table 343 describes the global Priority Flow Control (PFC) configuration options.

Table 343. Global Priority Flow Control Options (/cfg/cee/global/pfc)

Command Syntax and Usage
`pri <0-7>` Displays the 802.1p Priority PFC menu. To view menu options, see page 407.
`on` Globally turns PFC on.
`off` Globally turns PFC off.
`cur` Displays the current Priority Flow Control parameters.

/cfg/cee/global/pfc/pri <0-7>
802.1p Priority Flow Control Configuration

```
[Priority 1 Menu]
     ena      - Enable PFC on this priority queue
     dis      - Disable PFC on this priority queue
     desc     - Set a description string to identify the priority queue
     cur      - Display current PFC configuration
```

Table 344 describes the global Priority Flow Control (PFC) configuration options.

Table 344. Global PFC 802.1p Options (/cfg/cee/global/pfc/pri)

Command Syntax and Usage
`ena` 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.
`dis` Disables Priority Flow Control on the selected 802.1p priority.
`desc <1-31 characters>` Enter text to describe the 802.1p priority value.
`cur` Displays the current 802.1p Priority Flow Control parameters.

/cfg/cee/port <*port alias or number*>
CEE Port Configuration

```
[Port 1 CEE Configuration Menu]
     dcbx     - DCB Capability Exchange Protocol (DCBX) Menu
     pfc      - Priority Flow Control Menu
     cur      - Display current Port CEE configuration
```

Table 345 describes the Converged Enhanced Ethernet (CEE) port configuration options.

Table 345. CEE Port Options (/cfg/cee/port)

Command Syntax and Usage
`dcbx` Displays the DCB Capability Exchange Protocol (DCBX) menu for the selected port. To view menu options, see page 408.
`pfc` Displays the Priority Flow Control (PFC) menu for the selected port. To view menu options, see page 410.
`cur` Displays the current CEE port parameters.

/cfg/cee/port <*port alias or number*>/dcbx
DCBX Port Configuration

```
[Port EXT1 DCBX Config Menu]
     appadv   - Set Advertise flag for Application Protocol
     appwill  - Set Willing flag for Application Protocol
     etsadv   - Set Advertise flag for PG
     etswill  - Set Willing flag for PG
     pfcadv   - Set Advertise flag for PFC
     pfcwill  - Set Willing flag for PFC
     dis      - Disable DCBX
     ena      - Enable DCBX
     cur      - Display current port DCBX configuration
```

Data Center Bridging Capability Exchange (DCBX) protocol is used by Converged Enhanced Ethernet (CEE) networks to exchange advanced detection and configuration data.

Table 346 describes the port DCB Capability Exchange Protocol (DCBX) configuration options.

Table 346. Port DCBX Options (/cfg/cee/port x/dcbx)

Command Syntax and Usage
`appadv enable|disable` 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).
`appwill enable|disable` 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).
`etsadv enable|disable` Enables or disables DCBX ETS advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).
`etswill enable|disable` 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).
`pfcadv enable|disable` Enables or disables DCBX PFC advertisements of configuration data. When enabled, the Advertisement flag is set to 1 (advertise data to the peer device).
`pfcwill enable|disable` 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).
`dis` Disables DCBX on the port.
`ena` Enables DCBX on the port.
`cur` Displays the current DCBX parameters on the port.

/cfg/cee/port <*port alias or number*>/pfc
PFC Port Configuration

```
[Port EXT2 PFC Configuration Menu]
     pri      - 802.1p Priority PFC Menu
     on       - Turn ON PFC
     off      - Turn OFF PFC
     cur      - Display current PFC configuration
```

Table 347 describes the port Priority Flow Control (PFC) configuration options.

Table 347. Port PFC Options (/cfg/cee/port x/pfc)

Command Syntax and Usage
pri <*0-7*> Displays the 802.1p Priority PFC menu for the selected port. To view menu options, see page 410.
on Turns PFC on for the selected port.
off Turns PFC off for the selected port.
cur Displays the current PFC parameters for the selected port.

/cfg/cee/port <*port alias or number*>/pfc/pri <*0-7*>
802.1p PFC Port Configuration

```
[Priority 1 Menu]
     ena      - Enable PFC on this priority queue
     dis      - Disable PFC on this priority queue
     desc     - Set a description string to identify the priority queue
     cur      - Display current PFC configuration
```

Table 348 describes the port-level Priority Flow Control (PFC) configuration options.

Table 348. Port 802.1p PFC Options (/cfg/cee/port x/pfc/pri)

Command Syntax and Usage
ena 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.
dis Disables Priority Flow Control on the selected 802.1p priority.

Table 348. Port 802.1p PFC Options (/cfg/cee/port x/pfc/pri) (continued)

Command Syntax and Usage
`desc` *<1-31 characters>* Enter text to describe the 802.1p priority value.
`cur` Displays the current 802.1p Priority Flow Control parameters.

/cfg/fcoe
Fiber Channel over Ethernet Configuration

```
[Fiber Channel over Ethernet Configuration Menu]
     fips     - FCoE Initialization Protocol (FIP) Snooping Menu
     cur      - Display current FCOE configuration
```

Fiber Channel over Ethernet (FCoE) transports Fiber Channel frames over an Ethernet fabric. The CEE features and FCoE features allow you to create a lossless Ethernet transport mechanism.

Table 349 describes the FCoE configuration options.

Table 349. FCoE Options (/cfg/fcoe)

Command Syntax and Usage
`fips` Displays the FCoE Initialization Protocol (FIP) Snooping menu. To view menu options, see page 411.
`cur` Displays the current FCoE parameters.

/cfg/fcoe/fips
FIPS Configuration

```
[FIP Snooping Configuration Menu]
    port     - Port FIP snooping Menu
    on       - Globally turn FIP snooping ON
    off      - Globally turn FIP snooping OFF
    aclto    - Enable/Disable the removal of expired FCFs and FCOE ACLs
    cur      - Display current FIP snooping global 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 350 describes the FCoE Initialization Protocol (FIP) Snooping configuration options.

Table 350. FIP Snooping Options (/cfg/fcoe/fips)

Command Syntax and Usage
`port` *<port number>* Displays the FCoE Initialization Protocol (FIP) Snooping menu for the selected port. To view menu options, see page 412.
`on` Globally turns FIP Snooping on.
`off` Globally turns FIP Snooping off.
`aclto e|d` Enables or disables ACL time-out removal. When enabled, ACLs associated with expired FCFs and FCoE connections are removed from the system.
`cur` Displays the current FIP Snooping parameters.

/cfg/fcoe/fips/port *<port alias or number>*
FIPS Port Configuration

```
[Port 1 FIP Snooping Configuration Menu]
     fcfmode  - Set whether FCF is connected to this port
     ena      - Enable FIP snooping
     dis      - Disable FIP snooping
     cur      - Display current FIP snooping configuration
```

Table 344 describes the port FCoE Initialization Protocol (FIP) Snooping configuration options.

Table 351. Port FIP Snooping Options (/cfg/fcoe/fips/port)

Command Syntax and Usage
`fcfmode auto|on|off` Configures FCoE Forwarding (FCF) on the port, as follows: – `on`: Configures the port as a Fiber 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.
`ena` Enables FIP Snooping on the port. The default setting is `enabled`. **Note**: If IPv6 ACLs are assigned to the port, you cannot enable FCoE.

Table 351. Port FIP Snooping Options (/cfg/fcoe/fips/port) (continued)

Command Syntax and Usage
`dis` Disables FIP Snooping on the port.
`cur` Displays the current FIP Snooping parameters.

/cfg/rmon
Remote Monitoring Configuration

```
[RMON Menu]
     hist      - RMON History Menu
     event     - RMON Event Menu
     alarm     - RMON Alarm Menu
     cur       - Display current RMON configuration
```

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

Table 352 describes the Remote Monitoring (RMON) configuration menu options.

Table 352. Remote Monitoring (RMON) Menu Options (/cfg/rmon)

Command Syntax and Usage
`hist` *<1-65535>* Displays the RMON History Configuration menu. To view menu options, see page 414.
`event` *<1-65535>* Displays the RMON Event Configuration menu. To view menu options, see page 415.
`alarm` *<1-65535>* Displays the RMON Alarm Configuration menu. To view menu options, see page 415.
`cur` Displays the current RMON parameters.

/cfg/rmon/hist <*1-65535*>
RMON History Configuration Menu

```
[RMON History 2 Menu]
     ifoid    - Set interface MIB object to monitor
     rbnum    - Set the number of requested buckets
     intrval  - Set polling interval
     owner    - Set owner for the RMON group of statistics
     delete   - Delete this history and restore defaults
     cur      - Display current history configuration
```

Table 353 describes the RMON History Menu options.

Table 353. RMON History Menu Options (/cfg/rmon/hist)

Command Syntax and Usage
`ifoid` <*1-127 characters*> Configures the interface MIB Object Identifier. The IFOID must correspond to the standard interface OID, as follows: 1.3.6.1.2.1.2.2.1.1.x where x is the `ifIndex`
`rbnum` <*1-65535*> Configures the requested number of buckets, which is the number of discrete time intervals over which data is to be saved. The default value is 30. The maximum number of buckets that can be granted is 50.
`intrval` <*1-3600*> Configures the time interval over which the data is sampled for each bucket. The default value is 1800.
`owner` <*1-127 characters*> Enter a text string that identifies the person or entity that uses this History index.
`delete` Deletes the selected History index.
`cur` Displays the current RMON History parameters.

/cfg/rmon/event <1-65535>
RMON Event Configuration Menu

```
[RMON Event 2 Menu]
     descn    - Set description for the event
     type     - Set event type
     owner    - Set owner for the event
     delete   - Delete this event and restore defaults
     cur      - Display current event configuration
```

Table 354 describes the RMON Event Menu options.

Table 354. RMON Event Menu Options (/cfg/rmon/event)

Command Syntax and Usage
descn <1-127 characters> Enter a text string to describe the event.
type none|log|trap|both Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station.
owner <1-127 characters> Enter a text string that identifies the person or entity that uses this event index.
delete Deletes the selected RMON Event index.
cur Displays the current RMON Event parameters.

/cfg/rmon/alarm <1-65535>
RMON Alarm Configuration Menu

```
[RMON Alarm 2 Menu]
     oid      - Set MIB oid datasource to monitor
     intrval  - Set alarm interval
     sample   - Set sample type
     almtype  - Set startup alarm type
     rlimit   - Set rising threshold
     flimit   - Set falling threshold
     revtidx  - Set event index to fire on rising threshold crossing
     fevtidx  - Set event index to fire on falling threshold crossing
     owner    - Set owner for the alarm
     delete   - Delete this alarm and restore defaults
     cur      - Display current alarm configuration
```

The Alarm RMON group can track rising or falling values for a MIB object. The MIB object must be a counter, gauge, integer, or time interval. Each alarm index must correspond to an event index that triggers once the alarm threshold is crossed.

Table 355 describes the RMON Alarm Menu options.

Table 355. RMON Alarm Menu Options (/cfg/rmon/alarm)

Command Syntax and Usage
`oid` *<1-127 characters>* Configures an alarm MIB Object Identifier.
`intrval` *<1-65535>* Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The default value is 1800.
`sample abs|delta` Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: – `abs`–absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. – `delta`–delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
`almtype rising|falling|either` Configures the alarm type as rising, falling, or either (rising or falling).
`rlimit` *<-2147483647 - 2147483647>* Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.
`flimit` *<-2147483647 - 214748364)* Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.
`revtidx` *<1-65535>* Configures the rising alarm event index that is triggered when a rising threshold is crossed.
`fevtidx` *<1-65535>* Configures the falling alarm event index that is triggered when a falling threshold is crossed.
`owner` *<1-127 characters>* Enter a text string that identifies the person or entity that uses this alarm index.
`delete` Deletes the selected RMON Alarm index.
`cur` Displays the current RMON Alarm parameters.

/cfg/virt

Virtualization Configuration

```
[Virtualization Menu]
     evb      - Edge Virtual Bridge Menu
     vmpolicy - Virtual Machines Policy Configuration Menu
     vnic     - vNIC Configuration Menu
     vmcheck  - VM Check Menu
     vmgroup  - Virtual Machines Groups Menu
     vmprof   - Virtual Machine Profiles Menu
     vmware   - VMware-specific Settings Menu
     vmrmisc  - Miscellaneous VMready Configuration Menu
     enavmr   - Enable VMready
     disvmr   - Disable VMready
     cur      - Display all current virtualization settings
```

Table 356 describes the general virtualization configuration options. More detailed information is available in the following sections.

Table 356. Virtualization Configuration Options (/cfg/virt)

Command Syntax and Usage
`vmpolicy` Displays the Virtual Machines Policy menu. To view menu options, see page 418.
`vnic` Displays the Virtual NIC (vNIC) menu. To view menu options, see page 419.
`vmcheck` Displays the VM Check menu. To view menu options, see page 422.
`vmgroup` *<1-1024>* Displays the Virtual Machine Groups menu. To view menu options, see page 424.
`vmprof` Displays the Virtual Machine Profiles menu. To view menu options, see page 426.
`vmware` Displays the VMware settings menu. To view menu options, see page 428.
`enavmr` Enables VMready. The default setting is `disabled`.
`disvmr` Disables VMready.
`evb` Displays the Edge Virtual Bridge menu. To view menu options, see page 430.
`cur` Displays the current virtualization parameters.

/cfg/virt/vmpolicy
Virtual Machines Policy Configuration

```
[VM Policy Configuration Menu]
     vmbwidth -  VM Bandwidth Configuration Menu
```

Table 357 describes the Virtual Machines (VM) policy configuration options.

Table 357. VM Policy Options (/cfg/virt/vmpolicy)

Command Syntax and Usage
vmbwidth *<MAC address>* | *<UUID>* | *<name>* | *<IP address>* | *<index number>* Displays the bandwidth management menu for the selected Virtual Machine. Enter a unique identifier to select a VM.

/cfg/virt/vmpolicy/vmbwidth *<VM identifier>*
VM Policy Bandwidth Management

```
[VM Bandwidth Management Menu]
   txrate - Set VM Transmit Bandwidth (Ingress for switch)
   rxrate - Set VM Receive Bandwidth (Egress for switch)
   bwctrl - Enable/Disable VM Bandwidth Control
   delete - Delete VM bandwidth control Entry
   cur    - Display current VM bandwidth configuration
```

Table 358 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 358. VM Bandwidth Management Options (/cfg/virt/vmpolicy/vmbwidth)

Command Syntax and Usage
txrate *<64-10000000>* [32|64|128|256|512|1024|2048|4096] *<1-256>* The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096. The third value represents the ACL assigned to the transmission rate. The ACL is automatically, in sequential order, if not specified by the user. If there are no available ACLs, the TXrate cannot be configured. Each TXrate configuration reduces the number of available ACLs by one.
rxrate *<64-1000000>* [32|64|128|256|512|1024|2048|4096] The first value configures Committed Rate—the amount of bandwidth available to traffic transmitted from the switch to the VM, in kilobits per second. Enter the value in multiples of 64. The second values configures the maximum burst size, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

Table 358. VM Bandwidth Management Options (/cfg/virt/vmpolicy/vmbwidth) (continued)

Command Syntax and Usage
`bwctrl e|d` Enables or disables bandwidth control on the VM policy.
`delete` Deletes the bandwidth management settings from this VM policy.
`cur` Displays the current VM bandwidth management parameters.

/cfg/virt/vnic
Virtual NIC Configuration

```
[VNIC Global Configuration Menu]
     port     - Port vNIC Configuration Menu
     vnicgrp  - VNIC Group Configuration Menu
     on       - Globally turn vNIC feature ON
     off      - Globally turn vNIC feature OFF
     cur      - Display current vNIC configuration
```

Note: Table 359 describes the Virtual NIC (vNIC) configuration options.

Table 359. Virtual NIC Options (/cfg/virt/vnic)

Command Syntax and Usage
`port` *<port number>* Displays the port vNIC menu. To view menu options, see page 420.
`vnicgrp` *<1-32>* Displays the vNIC group menu. To view menu options, see page 421.
`on` Globally turns vNIC on.
`off` Globally turns vNIC off.
`cur` Displays the current vNIC parameters.

/cfg/virt/vnic/port <*port alias or number*>
vNIC Port Configuration

```
[Port 1 vNICs Menu]
     vnic      - VNIC Configuration Menu
     cur       - Display current port vNIC configuration
```

Table 360 describes the Virtual NIC (vNIC) port configuration options.

Table 360. vNIC Port Options (/cfg/virt/vnic/port)

Command Syntax and Usage
vnic <*1-4*> Displays the vNIC menu for the selected vNIC. To view menu options, see page 420.
cur Displays the current vNIC port parameters.

/cfg/virt/vnic/port <*port alias or number*>/vnic <*vNIC number*>
vNIC No. Port Configuration

```
[vNIC 1.1 Menu]
     bw        - Set maximum bandwidth of the vNIC
     ena       - Enable vNIC
     dis       - Disable vNIC
     cur       - Display current vNIC configuration
```

Table 361 describes the Virtual NIC (vNIC) port configuration options.

Table 361. Port vNIC Options (/cfg/virt/vnic/port/vnic)

Command Syntax and Usage
bw <*1-100*> Configures the maximum bandwidth allocated to this vNIC, in increments of 100 Mbps. For example: – 1 = 100 Mbps – 10 = 1000 Mbps
ena Enables the selected vNIC.
dis Disables the selected vNIC.
cur Displays the current vNIC port parameters.

/cfg/virt/vnic/vnicgrp <1-32>
Virtual NIC Group Configuration

```
[vNIC Group 1 Menu]
     vnicvlan - Set VLAN number to vNIC group
     failover - Enable/disable uplink failover
     addvnic  - Add vNIC to vNIC group
     remvnic  - Remove vNIC from vNIC group
     addport  - Add port to vNIC group
     remport  - Remove port from vNIC group
     addtrnk  - Add trunk to vNIC group
     remtrnk  - Remove trunk from vNIC group
     ena      - Enable vNIC group
     dis      - Disable vNIC group
     del      - Delete vNIC group
     cur      - Display current vNIC group configuration
```

Table 362 describes the Virtual NIC (vNIC) group configuration options.

Table 362. Port vNIC Group options (/cfg/virt/vnic/vnicgrp)

Command Syntax and Usage
`vnicvlan` *<VLAN number>* Assigns a VLAN to the vNIC group.
`failover e|d` Enables or disables uplink failover for the vNIC Group. Uplink Failover for the vNIC Group will disable only the affected vNIC links on the port. Other port functions continue to operate normally. The default setting is `disabled`.
`addvnic` *<vNIC ID>* Adds a vNIC to the vNIC Group. The vNIC ID is comprised of the port number and the vNIC number. For example: `intA1.1`
`remvnic` *<vNIC ID>* Removes the selected vNIC from the vNIC Group.
`addport` *<port number>* Adds the selected switch port to the vNIC Group.
`remport` *<port number>* Removes the selected switch port from the vNIC Group.
`addtrnk` *<trunk number>* Adds the selected trunk group to the vNIC Group.
`remtrnk` *<trunk number>* Removes the selected trunk group from the vNIC Group.
`ena` Enables the vNIC Group.

Table 362. Port vNIC Group options (/cfg/virt/vnic/vnicgrp)

Command Syntax and Usage
`dis` Disables the vNIC Group.
`del` Deletes the vNIC Group.
`cur` Displays the current vNIC Group parameters.

/cfg/virt/vmcheck
VM Check Configuration

```
[VM Check Settings Menu]
     action   - Actions to take for spoofed VMs
     acls     - Number of ACLs to use for spoofed macs
     trust    - Add a port to trusted ports
     notrust  - Remove a port from trusted ports
     cur      - Show current VM Check settings
```

Table 363 describes the the VM Check validation options used for MAC address spoof prevention.

Table 363. VM Check Options

Command Syntax and Usage
`action` Configures the actions taken when detecting MAC address spoofing. To view menu options, see page 423
`acls` *<1-256>* Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50.
`trust` *<ports>* Enables trusted ports for VM communication. By default, all ports are disabled.
`notrust` *<ports>* Disables trusted ports for VM communication.
`cur` Displays the current VM Check settings.

/cfg/virt/vmcheck/action
VM Check Actions Configuration

```
[VM Check actions settings Menu]
     basic    - Action to take in basic mode validation
     advanced - Action to take in advanced mode validation
     cur      - Show current VM Check Action settings
```

Table 364 describes the VM Check actions available for handling MAC address spoof attempts.

Table 364. VM Check Action Options

Command Syntax and Usage
`basic` *<log|link>* Sets up action taken when detecting MAC address spoofing in basic validation mode: – `log` registers a syslog entry – `link` registers a syslog entry and disables the corresponding switch port Default setting is `link`.
`advanced` *<log | acl | link>* Sets up action taken when detecting MAC address spoofing in advanced validation mode: – `log` registers a syslog entry – `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 Default setting is `acl`.
`cur` Displays the current VM Check actions settings.

/cfg/virt/vmgroup <1-1024>
VM Group Configuration

```
[VM group 1 Menu]
   vlan     - Set the group's vlan (only for groups with no VM profile)
   vmap     - Set VMAP for this group
   tag      - Enable vlan tagging on all VM group ports
   addvm    - Add a virtual entity to the group
   remvm    - Remove a virtual entity from the group
   validate - Sets secure mode for all VMs in this group
   addprof  - Add a VM profile to the group
   remprof  - Delete any VM profile associated with the group
   addport  - Add ports to the group
   report   - Remove ports from the group
   addtrunk - Add trunk to the group
   remtrunk - Remove trunk from the group
   addkey   - Add LACP trunk to the group
   remkey   - Remove LACP trunk from the group
   stg      - Assign VM group vlan to a Spanning Tree Group
   del      - Delete group
   cur      - Display current group configuration
```

Table 365 describes the Virtual Machine (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 365. VM Group Options (/cfg/virt/vmgroup)

Command Syntax and Usage
`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.
`vmap add|rem` *<VMAP number>* `intports|extports` Assigns the selected VLAN Map to this VM 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 264.
`tag e|d` Enables or disables VLAN tagging on ports in this VM group.
`addvm` *<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 (`/cfg/virt/vmware/vcspec`). The VM index number is found in the VM information dump (`/info/virt/vm/dump`). **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.

Table 365. VM Group Options (/cfg/virt/vmgroup) (continued)

Command Syntax and Usage
`remvm` *<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 (`/cfg/virt/vmware/vcspec`). The VM index number is found in the VM information dump (`/info/virt/vm/dump`).
`validate [disable|basic|advanced]` Configures MAC address spoof prevention for the VM group. – `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. – `disable` stops MAC address spoof prevention. Default setting is `disabled`.
`addprof` *<profile name (1-39 characters)>* Adds the selected VM profile to the VM group.
`remprof` Removes the VM profile assigned to the VM group.
`addport` *<port number or alias>* Adds the selected port to the VM group. **Note**: Add a port to a VM group only if no VMs on that port are members of the VM group.
`remport` *<port number or alias>* Removes the selected port from the VM group.
`addtrunk` *<trunk number>* Adds the selected trunk group to the VM group.
`remtrunk` *<trunk number>* Removes the selected trunk group from the VM group.
`addkey` *<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.
`remkey` *<1-65535>* Removes an LACP admin key from the VM group.

Table 365. VM Group Options (/cfg/virt/vmgroup) (continued)

Command Syntax and Usage
`stg` *<STG number>* Assigns the VM group VLAN to a Spanning Tree Group (STG).
`del` Deletes the VM group.
`cur` Displays the current VM group parameters.

/cfg/virt/vmprof
VM Profile Configuration

```
[VM Profiles Menu]
     create   - Create a VM profile
     edit     - Edit a VM profile
     cur      - Display details of all VM profiles
```

Configuration of VMs with the VM Agent requires the use of VM profiles, which ease the configuration and management of VM Agent-based VM groups. The VM profile contains a set of properties that will be configured on the Virtual Switch.

After a VM profile has been defined, it can be assigned to a VM group or exported to one or more VMware hosts.

Table 366 describes the VM Profiles configuration options.

Table 366. VM Profile options (/cfg/virt/vmprof)

Command Syntax and Usage
`create` *<profile name (1-39 characters)>* Defines a name for the VM profile. The switch supports up to 32 VM profiles.
`edit` *<profile name>* Displays the VM Profile Edit menu for the selected profile. To view menu options, see page 427.
`cur` Displays the current VM Profiles parameters.

/cfg/virt/vmprof/edit <*profile name*>

VM Profile Edit

```
[VM profile "myProfile" Menu]
   vlan     - Set the VM profile's VLAN ID
   shaping  - Set or delete the VM profile's traffic shaping parameters
   eshaping - Set or delete the VM profile's traffic eshaping parameters
   delete   - Delete this VM profile
   cur      - Show details of the current VM profile
```

Table 367 describes the VM Profile Edit options.

Table 367. Edit VM Profile options (/cfg/virt/vmprof/edit)

Command Syntax and Usage
`vlan` <*VLAN number*> Assigns a VLAN to the VM profile.
`shaping` [<*average (1-1000000000)*> <*burst (1-1000000000)*> <*peak (1-1000000000)*>] | `delete` 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.
`eshaping` [<*average (1-1000000000)*> <*burst (1-1000000000)*> <*peak (1-1000000000)*>] | `delete` Configures traffic eshaping 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.
`delete` Deletes the selected VM Profile.
`cur` Displays the current VM Profiles parameters.

/cfg/virt/vmware
VMWare Configuration

```
[VMware-specific Settings Menu]
  hbport    - Set ESX/ESXi server to vCenter heartbeat UDP port number
  vcspec    - Create, update or delete Virtual Center access information
  hello     - VM HELLO menu
  cur       - Display current VMware-specific settings
```

Table 368 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.

Table 368. VMware Options (/cfg/virt/vmware)

Command Syntax and Usage
`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.
`vcspec [<IP address>|[<username> noauth]|[delete]` 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)
`hello` Displays the VM Hello menu. To view menu options, see page 429.
`cur` Displays the current VMware parameters.

/cfg/virt/vmware/hello
VM Hello Configuration

```
[VM HELLO-specific settings Menu]
     ena      - Enable HELLO advertisements
     dis      - Disable HELLO advertisements
     addport  - Add PORT to HELLO
     rmport   - Remove PORT from HELLO
     haddr    - HELLO address
     htimer   - HELLO periodicity
     cur      - Show current HELLO settings
```

VM Hello configures the CDP (Cisco Discovery Protocol) advertisements sent periodically to VMware ESX hypervisors. Exchanging CDP message with ESX hypervisors, facilitates MAC address spoof prevention. Table 369 describes the VM Hello configuration options.

Table 369. VM Hello Configuration Options

Command Syntax and Usage
`ena` Enables CDP advertisements transmission. Default setting is disabled.
`dis` Disables CDP advertisements transmission.
`addport` *<ports>* Add ports to the list of ports that can transmit CDP advertisements.
`rmport` *<ports>* Remove ports from the list of ports that can transmit CDP advertisements
`haddr` *<IP_address>* Advertises a specific IP address instead of the default 0.0.0.0 IP.
`htimer` *<1-60>* Sets the number of seconds between successive CDP advertisements. Default value is 30.
`cur` Displays current VM Hello settings.

/cfg/virt/evb
Edge Virtual Bridge Configuration

```
[Edge Virtual Bridge Configuration Menu]
     vsidb    - Virtual Station Interface Type DataBase
     profile  - evb profile menu
     cur      - Show current EVB parameters
```

You can configure your switch to use Edge Virtual Bridging (EVB). These configuration commands are only available using the IBM Networking OS CLI and the Miscellaneous VMready Configuration Menu. Table 370 describes the Edge Virtual Bridge configuration options.

Note: EVB does not work in stacked mode.

Table 370. Edge Virtual Bridge Configuration Options

Command Syntax and Usage
`vsidb` Displays the Virtual Station Interface Type database menu. To view menu options, see page 430.
`profile` *<1-16>* Displays the EVB Profile menu. To view menu options, see page 431.
`cur` Displays the current EVB parameters.

/cfg/virt/evb/vsidb
VSI Type Database Configuration

```
[VSI Type DB 1 Menu]
     managrip -  Set VSI DB Manager IP
     port     -  Set VSI DB Manager Port
     docpath  -  Set VSI DB Document Path
     alltypes -  Set VSI DB Document Path
     interval -  Set VSI DB Update Interval
     cur      -  Display current VSI Type configuration
     reset    -  Reset VSIDB Info
```

Table 371 describes the Virtual Station Interface Type database configuration options.

Table 371. Virtual Station Interface Type Database Options

Command Syntax and Usage
`managrip` *<IP address>* Sets the Virtual Station Interface Type database manager IP address.
`port` *<1-65534>* Sets the Virtual Station Interface Type database manager port.

Table 371. Virtual Station Interface Type Database Options

Command Syntax and Usage
`docpath` *<URI path>* Sets the Virtual Station Interface Type database document path.
`alltypes` *<URI path>* Sets the Virtual Station Interface Type database document path for all types.
`cur` Displays the current Virtual Station Interface Type database parameters.
`reset` Resets the Virtual Station Interface Type database information to the default values.

/cfg/virt/evb/profile <1-16>
EVB Profile Configuration

```
[evb profile menu]
     rr       -  Enable/Disable VEPA Mode (Reflective Relay Capability)
     vsidisc  -  Enable/Disable VSI Discovery (ECP and VDP)
     cur      -  Display current configuration
```

Table 372 describes the Edge Virtual Bridge Profile configuration options.

Table 372. Edge Virtual Bridge Profile Configuration Options

Command Syntax and Usage
`rr enable|disable` Enables or disables VEPA mode (Reflective Relay capability).
`vsidisc enable|disable` Enables or disables VSI Discovery (ECP and VDP).
`cur` Displays the current EVB profile parameters.

/cfg/dump
Dump

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

```
Configuration# dump
```

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 TFTP or SFTP, as described on page 432.

/cfg/ptcfg <FTP/TFTP/SFTP server> <filename> <username>
Saving the Active Switch Configuration

When the ptcfg command is used, the switch's active configuration commands (as displayed using /cfg/dump) will be uploaded to the specified script configuration file on the FTP/TFTP/SFTP server. To start the switch configuration upload, at the Configuration# prompt, enter:

```
Configuration# ptcfg <FTP, TFTP or SFTP server> <filename> [mgt|extm|data]
```

Where *server* is the FTP/TFTP/SFTP server IPv4 address or hostname, and *filename* is the name of the target script configuration file. Select the port to use for the file transfer:

- mgt: Selects the internal management port. This is the default option.
- extm: Selects the external management port (EXT*x*)
- data: Selects a data port (EXT*x*).

Note: 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).

Note: If the FTP/TFTP/SFTP server is running SunOS or the Solaris operating system, the specified ptcfg file must exist prior to executing the ptcfg 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.

/cfg/gtcfg <FTP/TFTP/SFTP server> <filename>
Restoring the Active Switch Configuration

When the gtcfg 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. The configuration loaded using gtcfg is not activated until the apply command is used. If the apply command is found in the configuration script file loaded using this command, the apply action will be performed automatically.

To start the switch configuration download, at the Configuration# prompt, enter:

```
Configuration# gtcfg <FTP, TFTP or SFTP server> <filename> <username>
```

Where *server* is the FTP/TFTP/SFTP server IPv4 address or hostname, and *filename* is the name of the target script configuration file. Select the port to use for the file transfer:

- mgt: Selects the internal management port. This is the default option.
- extm: Selects the external management port (EXT*x*)
- data: Selects a data port (EXT*x*).

Chapter 6. The Operations Menu

The Operations Menu is generally used for commands that affect switch performance immediately, but do not alter permanent switch configurations. For example, you can use the Operations Menu 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.

/oper
Operations Menu

```
[Operations Menu]
     port     - Operational Port Menu
     fcoe     - Operational Fiber Channel Over Ethernet Menu
     vrrp     - Operational Virtual Router Redundancy Menu
     ip       - Operational IP Menu
     prm      - Protected Mode Menu
     sys      - Operational System Menu
     virt     - Virtualization Operations Menu
     passwd   - Change current user password
     clrlog   - Clear syslog messages
     tnetsshc - Close all telnet/SSH connections
     conlog   - Enable/disable session console logging
     cfgtrk   - Track last config change made
     ntpreq   - Send NTP request
     swkey    - Software License Menu
```

The commands of the Operations Menu enable you to alter switch operational characteristics without affecting switch configuration.

Table 373. Operations Menu (/oper)

Command Syntax and Usage
`port` *<port alias or number>* Displays the Operational Port Menu. To view menu options, see page 435.
`fcoe` Displays the Fiber Channel over Ethernet (FCoE) Operations Menu. To view menu options, see page 436.
`vrrp` Displays the Operational Virtual Router Redundancy Menu. To view menu options, see page 437.
`ip` Displays the IP Operations Menu, which has one sub-menu/option, the Operational Border Gateway Protocol Menu. To view menu options, see page 438.
`prm` Displays the Protected Mode menu. To view menu options, see page 439.

Table 373. Operations Menu (/oper) (continued)

Command Syntax and Usage
`sys` Displays the Operational System menu. To view menu options, see page 440.
`virt` Displays the Virtualization Operations Menu. To view menu options, see page 440.
`passwd` *<1-128 characters>* Allows the user to change the password. You need to enter the current password in use for validation.
`clrlog` Clears all Syslog messages.
`tnetsshc` Closes all open Telnet and SSH connections.
`conlog enable|disable` Enables of disables console logging of the current session.
`cfgtrk` Displays a list of configuration changes made since the last `apply` command. Each time the `apply` command is sent, the configuration-tracking log is cleared.
`ntpreq` Allows the user to send requests to the NTP server.
`swkey` Displays the Software Key menu. To view menu options, see page 447.

/oper/port <*port alias or number*>
Operations-Level Port Options Menu

```
[Operations Port INTA1 Menu]
     8021x    - 8021.x Menu
     rmon     - Enable/disable RMON for port
     ena      - Enable port
     dis      - Disable port
     lena     - Enable FDB Learning
     ldis     - Disable FDB Learning
     cur      - Current port state
```

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

Table 374. Operations-Level Port Menu Options (/oper/port)

Command Syntax and Usage
`8021x` Displays the 802.1X Port Menu. To view menu options, see page 436.
`rmon e|d` Enables or disables Remote Monitoring (RMON) for the port. The default setting is `disabled`.
`ena` Temporarily enables the port. The port will be returned to its configured operation mode when the switch is reset.
`dis` Temporarily disables the port. The port will be returned to its configured operation mode when the switch is reset.
`lena` Temporarily enables FDB learning on the port.
`ldis` Temporarily disables FDB learning on the port.
`cur` Displays the current settings for the port.

/oper/port <*port alias or number*>/8021x
Operations-Level Port 802.1X Options Menu

```
[802.1X Operation Menu]
     reset    - Reinitialize 802.1X access control on this port
     reauth   - Initiate reauthentication on this port now
```

Operations-level port 802.1X options are used to temporarily set 802.1X parameters for a port.

Table 375. Operations-Level Port 802.1X Menu Options (/oper/port x/8021x)

Command Syntax and Usage
`reset` Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration: – `force unauth` - the port is placed in unauthorized state, and traffic is blocked. – `auto` - the port is placed in unauthorized state, then authentication is initiated. – `force auth` - the port is placed in authorized state, and authentication is not required.
`reauth` Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as `auto`.

/oper/fcoe
Operations-Level FCoE Menu

```
[Operational FCOE Menu]
     fips     - Operational FIP Snooping Menu
```

Table 376. Operations-Level FCoE Options (/oper/fcoe)

Command Syntax and Usage
`fips` Displays the FCoE Initialization Protocol Snooping operations menu.

/oper/fcoe/fips
FCoE FIP Snooping Operations

```
[FIP Snooping Operational Menu]
     delfcf   - Delete an FCF entry and the associated ACLs from the database
```

Table 377. FIP Snooping Operations (/oper/fcoe/fips)

Command Syntax and Usage
`delfcf` *<MAC address>* `[VLAN no.]` Deletes the selected FCoE Forwarder (FCF), and any associated ACLs.

/oper/vrrp
Operations-Level VRRP Options Menu

```
[VRRP Operations Menu]
       back   - Set virtual router to backup
```

Table 378. Operations-Level VRRP Menu Options (/oper/vrrp)

Command Syntax and Usage
`back` *<virtual router number (1-255)>* Forces the specified master virtual router on this switch into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases: – This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same) – This switch's virtual router has a higher priority and preemption is enabled. – There are no other virtual routers available to take master control.

/oper/ip
Operations-Level IP Options Menu

```
[IP Operations Menu]
      bgp     - Operational Border Gateway Protocol Menu
```

Table 379. Operations-Level IP Menu Options (/oper/ip)

Command Syntax and Usage
`bgp` Displays the Border Gateway Protocol Operations Menu. To view the menu options see page 438.

/oper/ip/bgp
Operations-Level BGP Options Menu

```
[Border Gateway Protocol Operations Menu]
      start   - Start peer session
      stop    - Stop peer session
      cur     - Current BGP operational state
```

Table 380. Operations-Level BGP Menu Options (/oper/ip/bgp)

Command Syntax and Usage
`start` *<peer number>* Starts the peer session.
`stop` *<peer number>* Stops the peer session.
`cur` Displays the current BGP operational state.

/oper/prm

Protected Mode Options Menu

```
[Protected Mode Menu]
    mgt  - Enable/disable local control of external management
    ext  - Enable/disable local control of external ports
    fact - Enable/disable local control of factory default reset
    mif  - Enable/disable local control of Mgmt VLAN interface
    on   - Turn on/alter protected mode by applying enabled features
    off  - Turn off protected mode by removing all features
    cur  - Display current PRM configuration
```

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

Table 381. Protected Mode Options (/oper/prm)

Command Syntax and Usage
`mgt enable|disable` 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.
`ext enable|disable` 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.
`fact enable|disable` 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.
`mif enable|disable` 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.
`on` Turns Protected Mode `on`. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.

Table 381. Protected Mode Options (/oper/prm) (continued)

Command Syntax and Usage
`off` Turns Protected Mode `off`. When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.
`cur` Displays the current Protected Mode configuration.

/oper/sys
System Operations Menu

```
[Operational System Menu]
     i2c      - System I2C
     srvled   - Enable/disable Service Required LED
```

I2C device commands are to be used only by Technical Support personnel.

/oper/virt
Virtualization Operations

```
[Virtualization Operations Menu]
     vmware   - VMware Operations Menu
     vmcheck  - VMcheck Operations Menu
     evb      - EVB Operations Menu
```

Table 382 describes general virtualization operations options. More details are available in the following sections.

Table 382. Virtualization Options (/oper/virt)

Command Syntax and Usage
`vmware` Displays the VMware Operations menu. To view the menu options see page 441.
`vmcheck` Displays the VMcheck Operations menu. To view the menu options see page 445.
`evb` Displays the Edge Virtual Bridge operations menu. To view the menu options see page 446.

/oper/virt/vmware
VMware Operations

```
[VMware Operations Menu]
     dvswitch - VMware dvSwitch Operations
     dpg      - VMware distributed port group operation
     addpg    - Add a port group to a Host
     addvsw   - Add a Vswitch to a Host
     delpg    - Delete a port group from a Host
     delvsw   - Delete a Vswitch from a Host
     export   - Create or update a VM profile on one or more Hosts
     scan     - Perform a VM Agent scan operation now
     vmacpg   - Change a VM NIC's port group
     updpg    - Update a port group on a Host
```

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

Table 383. VMware Operations (/oper/virt/vmware)

Command Syntax and Usage
`dvswitch` Displays the Distributed vSwitch Operations menu. To view the menu options see page 443.
`dpg` Displays the Distributed Port Groups Operations menu. To view the menu options see page 444.
`addpg` [*<Port Group name> <host ID> <Vswitch name> <VLAN number> <shaping-enabled> <average-Kbps> <burst-KB> <peak-Kbps>*] Adds a Port Group to a VMware host. You are prompted for the following information: – Port Group name – VMware host ID (Use host UUID, host IP address, or host name.) – Virtual Switch name – VLAN ID of the Port Group – Whether to enable the traffic-shaping profile (`y` or `n`). If you choose `y` (yes), you are prompted to enter the traffic shaping parameters.
`addvsw` *<host ID> <Virtual Switch name>* Adds a Virtual Switch to a VMware host. Use one of the following identifiers to specify the host: – UUID – IP address – Host name

Table 383. VMware Operations (/oper/virt/vmware) (continued)

Command Syntax and Usage
`delpg` *<Port Group name> <host ID>* Removes a Port Group from a VMware host. Use one of the following identifiers to specify the host: – UUID – IP address – Host name
`delvsw` *<host ID> <Virtual Switch name>* Removes a Virtual Switch from a VMware host. Use one of the following identifiers to specify the host: – UUID – IP address – Host name
`export` *<VM profile name> <VMware host ID (one per line, 'null' to end)> <Virtual Switch name>* Exports a VM Profile to one or more VMware hosts. This command allows you to distribute a VM Profile to VMware hosts. Use one of the following identifiers to specify each host: – UUID – IP address – Host name The switch displays a list of available Virtual Switches. You may enter a VSwitch name from the list, or enter a new name to create a new Virtual Switch.
`scan` Performs a scan of the VM Agent, and updates VM information.
`vmacpg` *<MAC address> <Port Group name>* Changes a VM NIC's configured Port Group.
`updpg` *<Port Group name> <host ID> <VLAN number>* `[`*<shaping enabled> <average (1-1000000000)> <burst (1-1000000000)> <peak (1-1000000000)>*`]` Updates a VMware host's Port Group parameters. Use one of the following identifiers for the host ID: – UUID – IP address – Host name Enter the traffic shaping parameters as follows: – Shaping enabled – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters.

/oper/virt/vmware/dvswitch
Distributed vSwitch Operations

```
[VMware dvSwitch operations Menu]
     add      - Add a dvSwitch to a DataCenter
     del      - Delete a dvSwitch from a DataCenter
     addhost  - Add a host to a dvSwitch
     remhost  - Remove a host from a dvSwitch
     adduplnk - Add a physical NIC to dvSwitch uplink ports
     remuplnk - Remove a physical NIC from dvSwitch uplink ports
```

Table 384 describes distributed vSwitch operations.

Table 384. Distributed vSwitch Options (/oper/virt/vmware/dvswitch)

Command Syntax and Usage
`add` *<datacenter name> <dvSwitch name> <vSwitch version>* Adds a distributed vSwitch to a datacenter.
`del` *<datacenter name> <dvSwitch name>* Deletes a distributed vSwitch from a datacenter.
`addhost` *<dvSwitch name> <host UUID, IP address, or name>* Adds a host to a distributed vSwitch.
`remhost` *<dvSwitch name> <host UUID, IP address, or name>* Removes a host from a distributed vSwitch.
`adduplink` *<dvSwitch name> <host UUID, IP address, or name> <uplink name>* Adds a NIC to the distributed vSwitch, to use as an uplink.
`remuplink` *<dvSwitch name> <host UUID, IP address, or name> <uplink name>* Removes an uplink NIC from the distributed vSwitch.

/oper/virt/vmware/dpg
Distributed Port Group Operations

```
[VMware distributed port group operations Menu]
     add      - Add a port group to a dvSwitch
     addmac   - Add a VM NIC to a port group
     update   - Update a port group on a dvSwitch
     del      - Delete a port group from a dvSwitch
```

Table 385 describes distributed port group operations.

Table 385. Distributed Port Group Options (/oper/virt/vmware/dpg)

Command Syntax and Usage

`add` *<port group name> <dvSwitch name> <VLAN number>*
`[ingress-shaping-enabled` *<average Kbps> <burst KB> <peak Kbps>*`]`
`[egress-shaping-enabled` *<average Kbps> <burst KB> <peak Kbps>*`]`
Adds a port group to a distributed vSwitch. Follow the prompts to complete the operation.
Note: Ingress shaping and egress shaping parameters are optional.

`addmac` *<vNIC MAC> <port group name>* Adds a vNIC to a distributed port group.

`update` *<port group name> <dvSwitch name> <VLAN number>*
`[ingress-shaping-enabled` *<average Kbps> <burst KB> <peak Kbps>*`]`
`[egress-shaping-enabled` *<average Kbps> <burst KB> <peak Kbps>*`]`
Updates the parameters of a distributed port group. Follow the prompts to complete the operation.
Note: Ingress shaping and egress shaping parameters are optional.

`del` *<port group name> <dvSwitch name>* Deletes a port group from a distributed vSwitch.

/oper/virt/vmcheck/acl
VMcheck ACL Operations

```
[VMcheck ACL operations Menu]
     remall   - Delete all VMcheck ACLs
     remmac   - Delete an ACL by mac address [and port]
     remport  - Delete all ACLs installed on a port
```

Table 386 describes ACL removal operations.

Table 386. ACL removal Options (/oper/virt/vmcheck/acl)

Command Syntax and Usage
`remall` Deletes all ACLs
`remmac` *<ACL MAC address>* `[`*<port number>*`]` Removes ACLs based on the MAC address and, optionally, based on port number.
`remport` *<port number>* Removes ACLs based on port number

/oper/virt/evb
Edge Virtual Bridging Operations

```
[EVB Operations Menu]
     cleanvms - Clean VM Associations
     dbupdate - Update VSI DataBase
     dbclean  - Clean VSI DataBase
```

Use these commands to perform minor adjustments to Edge Virtual Bridging (EVB) operations. Use these commands to perform Virtual Switch operations directly from the switch.

Note: These commands are only valid in the IBM Networking OS CLI interface.

Table 387. EVB Operations (/oper/virt/evb)

Command Syntax and Usage
`cleanvms [port` <*Port number*>`|MAC` <*MAC ID*>`|vlan` <*VLAN number*> `typeid` <*type ID number*>`]` Cleans VM associations. If no argument is given, it erases all VM associations.
`dbupdate` Updates the VSI database
`dbclean` Cleans the VSI database

/oper/swkey
Software Key Menu

```
[Software License Menu]
     fodkey   - Feature on Demand Key Menu
```

The commands in this menu configure the software license key feature.

Table 388. Software Key options (/oper/swkey)

Command Syntax and Usage
`fodkey` Displays the Feature on Demand Key menu.

/oper/swkey/fodkey
Feature on Demand Options Menu

```
[Feature on Demand Key  Menu]
     enakey   - Enable FoD Key
     rmkey    - Remove FoD Key
     ptkey    - Upload FoD Key File
     invkeys  - Upload inventory installed activation keys
```

Use the commands in this menu 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.

Table 389. Feature on Demand Key Options (/oper/swkey/fodkey)

Command Syntax and Usage
`enakey` *<hostname or IP address> <file name>* [*<SFTP username>*] Allows you to unlock 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.
`rmkey` *<feature name>* Removes the specified software feature.
`ptkey` *<hostname or IP address> <file name>* [*<SFTP username>*] Loads the specified key file to a server.
`invkeys` *<hostname or IP address> <file name>* [*<SFTP username>*] Loads key code inventory information to a server.

Chapter 7. The Boot Options Menu

To use the Boot Options Menu, you must be logged in to the switch as the administrator. The Boot Options Menu provides 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/SFTP

In addition to the Boot Menu, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to “Switch Images and Configuration Files” on page 495.

/boot
Boot Menu

```
[Boot Options Menu]
     sched    - Scheduled Switch Reset Menu
     image    - Select software image to use on next boot
     conf     - Select config block to use on next boot
     netboot  - NetBoot and NetConfig menu
     qsfp40g  - QSFP 40G Ports Menu
     mode     - Select CLI mode to use on next boot
     prompt    - Prompt for selectable boot mode
     gtimg    - Download new software image via TFTP
     ptimg    - Upload selected software image via TFTP
     reset    - Reset switch [WARNING: Restarts Spanning Tree]
     cur      - Display current boot options
```

Each of these options is discussed in greater detail in the following sections.

/boot/sched
Scheduled Reboot Menu

```
[Boot Schedule Menu]
     set      - Set switch reset time
     cancel   - Cancel pending switch reset
     cur      - Display current switch reset schedule
```

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 390. Boot Scheduling Options (/boot/sched)

Command Syntax and Usage
`set` Defines the reboot schedule. Follow the prompts to configure schedule options.
`cancel` Cancels the next pending scheduled reboot.
`cur` Displays the current reboot scheduling parameters.

/boot/netboot
Netboot Configuration Menu

```
[Netboot configuration Menu]
     ena      - Enable netconfig
     dis      - Disable netconfig
     tftpaddr - TFTP Server IP address
     cfgfile  - Location of config file on tftp server
     cur      - Display current 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 391. Netboot Options (/boot/netboot)

Command Syntax and Usage
`ena` Enables Netboot. When enabled, the switch boots into factory-default configuration, and attempts to download a new configuration file.
`dis` Disables Netboot.
`tftpaddr` *<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.
`cfgfile` *<1-31 characters>* Defines the file path for the configuration file on the TFTP server. For example: `/directory/sub/config.cfg`
`cur` Displays the current Netboot parameters.

/boot/qsfp40g

QSFP+ Port Configuration Menu

```
[QSFP 40G Mode Menu]
     add      - Enable 40G mode for QSFP ports, effective after reboot
     rem      - Disable 40G mode for QSFP ports, effective after reboot
     cur      - Display 40G mode ports configuration
```

Table 392. QSFP Port Options

Command Syntax and Usage
`add` *<EXT15, EXT19>* Enables 40GbE mode on the selected QSFP+ ports. When enabled, each QSFP+ port is set as a single 40GbE port. You must reboot the switch for this change to take effect.
`rem` *<EXT15, EXT19>* Disables 40GbE mode on the selected QSFP+ ports. When disabled, each QSFP+ port is configured to breakout into four 10GbE ports. You must reboot the switch for this change to take effect.
`cur` Displays the current QSFP+ port settings.

Updating the Switch Software Image

The switch software image is the executable code running on the CN4093 10Gb Converged Scalable Switch (CN4093). 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 switch, go to:

http://www.ibm.com/systems/support

On the support site, click on software updates. On the switch, use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Place the new image onto a FTP, TFTP or SFTP server on your network, or on a local computer.
- Transfer the new image to your switch.
- Select 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.

Using the BBI

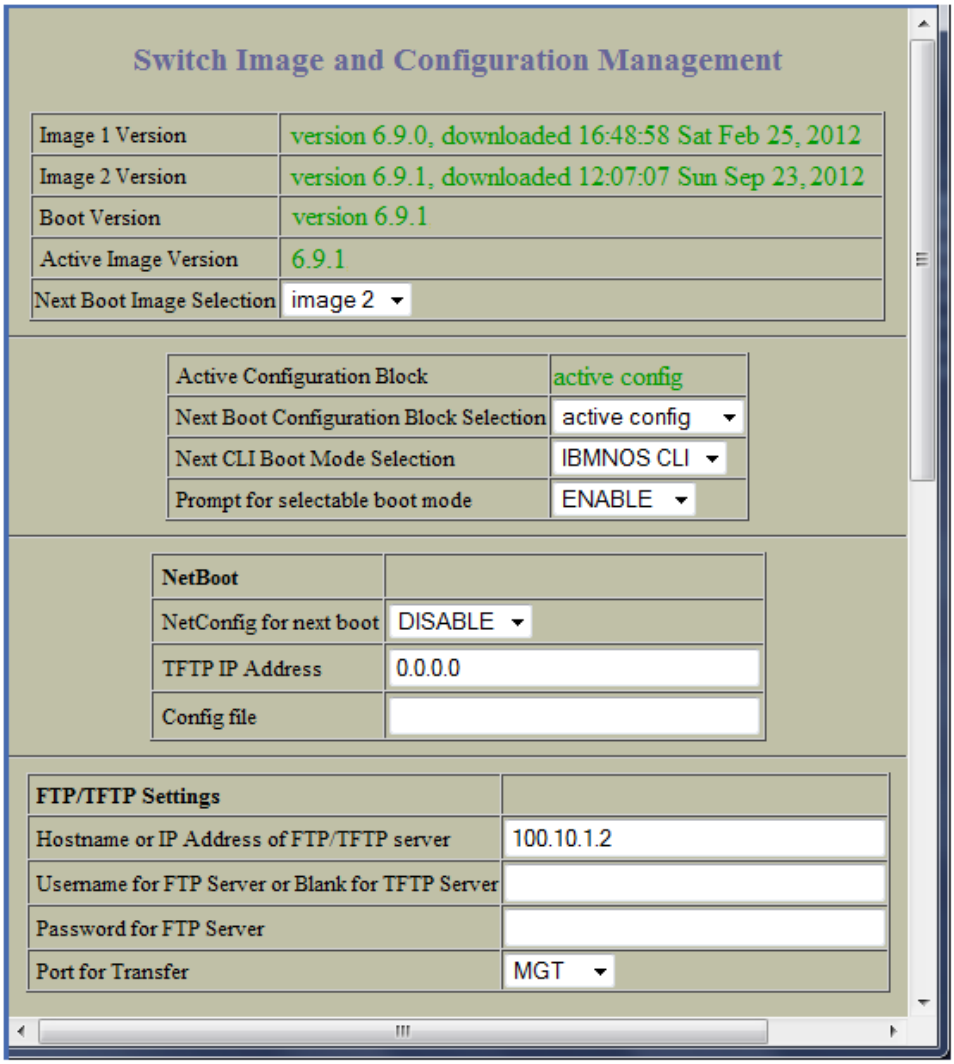
You can use the Browser-Based Interface to load software onto the CN4093. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- SFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. Click the Configure context button in the toolbar.
2. In the Navigation Window, select System > Config/Image Control.

The Switch Image and Configuration Management page appears.



3. If you are loading software from your computer (HTTP client), go to Step 4.

   If you are loading software from a FTP/TFTP/SFTP server, enter the server's information in the FTP/TFTP/SFTP Settings section.

4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
   - If you are loading software from a FTP/TFTP/SFTP server, enter the file name and click Get Image.
   - If you are loading software from your computer, click Browse.
     In the File Upload Dialog, select the file and click OK.
     Click Download via Browser.

Once the image has loaded, the page refreshes to show the new software.

Using the CLI

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

- The image or boot software loaded on a FTP/TFTP/SFTP server on your network
- The hostname or IPv4/IPv6 address of the FTP/TFTP/SFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames. See "Domain Name System Configuration Menu" on page 369.

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

1. At the `Boot Options#` prompt, enter:

```
Boot Options# gtimg
```

2. Enter the name of the switch software to be replaced:

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. Enter the hostname or IPv4/IPv6 address of the FTP, TFTP or SFTP server.

```
Enter hostname or IP address of SFTP/FTP/TFTP server: <name or IP address>
```

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

```
Enter name of file on SFTP/FTP/TFTP server: <filename>
```

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

5. Enter your username for the server, if applicable.

```
Enter username for SFTP/FTP server or hit return for TFTP server: <username> or
<Enter>
```

6. Enter the switch port to use for the file transfer. The default option is `mgt`.

```
Enter the port to use for downloading the image
["mgt"|"extm"|"data"]:
```

7. The system prompts you to confirm your request.

You will 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. At the `Boot Options#` prompt, enter:

```
Boot Options# image
```

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

   The system informs you of which image is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use switch software "image1" on next reset.
Specify new image to use on next reset ["image1"/"image2"]:
```

Uploading a Software Image from Your Switch

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

1. At the `Boot Options#` prompt, enter:

```
Boot Options# ptimg
```

2. The system prompts you for information. Enter the desired image:

```
Enter name of switch software image to be uploaded
["image1"|"image2"|"boot"]: <image>
```

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

```
Enter hostname or IP address of SFTP/FTP/TFTP server: <name or IP address>
```

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

```
Enter name of file on SFTP/FTP/TFTP server: <filename>
```

5. Enter the switch port to use for the file transfer. The default option is `mgt`.

```
Enter the port to use for uploading the image
["mgt"|"extm"|"data"]:
```

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

```
image2 currently contains Software Version 7.5.0
 that was downloaded at 0:23:39 Thu Jan  4, 2012.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on SFTP/FTP/TFTP server 192.1.1.1. over the MGT port.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the CN4093, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform the `save` command, your new configuration changes are placed in the *active* configuration block. The previous configuration is copied into the *backup* configuration block.

There is also a *factory* configuration block. This holds the default configuration set by the factory when your CN4093 was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured CN4093 is moved to a network environment where it will be re-configured for a different purpose.

Note: You also can use Netboot to automatically download a configuration file when the switch reboots. For more details, see "Netboot Configuration Menu" on page 451.

Use the following procedure to set which configuration block you want the switch to load the next time it is reset:

1. At the `Boot Options#` prompt, enter:

```
Boot Options# conf
```

2. Enter the name of the configuration block you want the switch to use:

   The system informs you of which configuration block is currently set to be loaded at the next reset, and prompts you to enter a new choice:

```
Currently set to use active configuration block on next reset.
Specify new block to use ["active"/"backup"/"factory"]:
```

Resetting the Switch

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

Note: Resetting the switch causes the Spanning Tree Group to restart. This process can be lengthy, depending on the topology of your network.

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

Accessing the ISCLI

The default command-line interface for the CN4093 is the menu-based CLI. To access the ISCLI, enter the following command and reset the CN4093:

```
Main# boot/mode iscli
```

To access the menu-based CLI, enter the following command from the ISCLI and reload the CN4093:

```
Switch (config)# boot cli-mode ibmnos-cli
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

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 ..............................

1 - Change booting image
2 - Change configuration block
3 - Boot in recovery mode (tftp and xmodem download of images to
    recover switch)
4 - Xmodem download (for boot image only - use recovery mode for
    application images)
5 - Reboot
6 - Exit

Please choose your menu option: 3
```

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 a software image recovery, press 3 and follow the screen prompts.
- To perform an Xmodem download (boot image only), press 4 and follow the screen prompts.
- To exit the Boot Management menu, press 6. 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 **Boot in recovery mode**. You will see the following display:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

   – If you choose option **x** (Xmodem serial download), go to step 5.
   – If you choose option **t** (TFTP download), go to step 6.

5. **Xmodem download**: 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.
   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.
```

   c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

   d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

6. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter
'q' to quit):
IP addr    :
Server addr:
Netmask    :
Gateway    :
Image Filename:
```

a. Enter the required information and press <**Enter**>.

b. You will see a display similar to the following:

```
        Host IP    : 10.10.98.110
        Server IP  : 10.10.98.100
        Netmask    : 255.255.255.0
        Broadcast  : 10.10.98.255
        Gateway    : 10.10.98.254
Installing image 6.8.3_OS.img from TFTP server 10.10.98.100
```

c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

7. Image recovery is complete. Perform one of the following steps:
   – Press **r** to reboot the switch.
   – Press **e** to exit the Boot Management menu
   – Press the Escape key (<**Esc>**) to re-display the Boot Management menu.

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 8. The Maintenance Menu

The Maintenance Menu is used to manage dump information and forward database information. It also includes a debugging menu to help with troubleshooting.

/maint
Maintenance Menu

Note: To use the Maintenance Menu, you must be logged in to the switch as the administrator.

```
[Maintenance Menu]
     sys      - System Maintenance Menu
     fdb      - Forwarding Database Manipulation Menu
     debug    - Debugging Menu
     dcbx     - DCBX Debug Menu
     lldp     - LLDP Cache Manipulation Menu
     arp      - ARP Cache Manipulation Menu
     route    - IP Route Manipulation Menu
     igmp     - IGMP Multicast Group Menu
     mld      - MLD Multicast Group Menu
     lacp     - LACP Menu
     stp      - STP Maint Menu
     tacacs+  - TACACS+ Maint Menu
     nbrcache - IP6 NBR Cache Manipulation Menu
     route6   - IP6 Route Manipulation Menu
     uudmp    - Uuencode FLASH dump
     ptdmp    - Upload FLASH dump via FTP/SFTP/TFTP
     ptlog    - Upload file via SFTP/TFTP
     cldmp    - Clear FLASH dump
     tsdmp    - Tech support dump
     pttsdmp  - Upload tech support dump via FTP/SFTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the CN4093 10Gb Converged Scalable Switch (CN4093) 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.

Table 393. Maintenance Menu (/maint)

Command Syntax and Usage
`sys` Displays the System Maintenance Menu. To view menu options, see page 465.
`fdb` Displays the Forwarding Database Manipulation Menu. To view menu options, see page 466.
`debug` Displays the Debugging Menu. To view menu options, see page 467.

Table 393. Maintenance Menu (/maint)

Command Syntax and Usage
`dcbx` Displays the DCBX Debugging Menu. To view menu options, see page 468
`lldp` Displays the LLDP Cache Manipulation menu. To view menu options, see page 469.
`arp` Displays the ARP Cache Manipulation menu. To view menu options, see page 470.
`route` Displays the IP Route Manipulation menu. To view menu options, see page 471.
`igmp` Displays the IGMP Maintenance menu. To view menu options, see page 472.
`mld` Displays the Multicast Listener Discovery (MLD) Maintenance menu. To view menu options, see page 474.
`lacp` Displays the Link Aggregation Control Protocol Maintenance menu. To view menu options, see page 475.
`stp` Displays the Spanning Tree Maintenance menu. STP maintenance commands are reserved for Technical Support Personnel.
`tacacs+` Displays the TACACS+ Maintenance menu. TACACS+ maintenance commands are reserved for Technical Support Personnel.
`nbrcache` Displays the IPv6 Neighbor Cache Manipulation menu. To view menu options, see page 475.
`route6` Displays the IPv6 Route Manipulation menu. To view menu options, see page 476.
`uudmp` Displays dump information in uuencoded format. For details, see page 476.
`ptdmp` *<host name> <file name>* Saves the system dump information via FTP/TFTP/SFTP. For details, see page 477.
`ptlog` Saves the system log file (SYSLOG) via SFTP/TFTP.

Table 393. Maintenance Menu (/maint)

Command Syntax and Usage
`cldmp` Clears dump information from flash memory. For details, see page 477.
`tsdmp` Dumps all CN4093 information, statistics, and configuration.You can log the tsdump output into a file.
`pttsdmp` Redirects the technical support dump (tsdmp) to an external FTP/TFTP/SFTP server.

/maint/sys
System Maintenance Menu

This menu is reserved for use by IBM Service Support. The options are used to perform system debugging.

```
[System Maintenance Menu]
      flags   - Set NVRAM flag word
      tmask   - Set MP trace mask word
```

Table 394. System Maintenance Menu Options (/maint/sys)

Command Syntax and Usage
`flags` *<new NVRAM flags word as 0xXXXXXXXX>* This command sets the flags that are used for debugging purposes by Technical Support personnel.
`tmask` *<new trace mask word as 0xXXXXXXXX>* [p] This command sets the trace mask that is used for debugging purposes by Technical Support personnel.

/maint/fdb
Forwarding Database Maintenance Menu

```
[FDB Manipulation Menu]
     find     - Show a single FDB entry by MAC address
     port     - Show FDB entries for a single port
     trunk    - Show FDB entries for a single trunk
     vlan     - Show FDB entries for a single VLAN
     dump     - Show all FDB entries
     del      - Delete an FDB entry
     clear    - Clear entire FDB
```

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

Table 395. FDB Manipulation Menu Options (/maint/fdb)

Command Syntax and Usage
`find` *<MAC address>* [*<VLAN number>*] 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 one of the following formats: – `xx:xx:xx:xx:xx:xx` (such as `08:00:20:12:34:56`) – `xxxxxxxxxxxx` (such as `080020123456`)
`port` *<port alias or number>* Displays all FDB entries for a particular port.
`trunk` *<trunk group number>* Displays all FDB entries for a particular Trunk Group.
`vlan` *<VLAN number>* Displays all FDB entries on a single VLAN.
`dump` Displays all entries in the Forwarding Database. For details, see page 34.
`del` *<MAC address>* [*<VLAN number>*] Removes a single FDB entry.
`clear` Clears the entire Forwarding Database from switch memory.

/maint/debug
Debugging Menu

```
[Miscellaneous Debug Menu]
     tbuf     - Show MP trace buffer
     dumpbt   - Dump backtrace log
     snap     - Show MP snap (or post-mortem) trace buffer
     clrcfg   - Clear all flash configs
     sec      - IP security Debug Menu
     gea      - GEA 5690 Menu
```

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

- 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 Service Support personnel.

Table 396. Miscellaneous Debug Menu Options (/maint/debug)

Command Syntax and Usage

`tbuf`
Displays the Management Processor trace buffer. Header information similar to the following is shown:
`MP trace buffer at 13:28:15 Fri May 30, 2008; mask: 0x2ffdf748`
The buffer information is displayed after the header.

`dumpbt` Displays the backtrace log.
`snap` Displays the Management Processor snap (or post-mortem) trace buffer. This buffer contains information traced at the time that a reset occurred.
`clrcfg` Deletes all flash configuration blocks.
`sec` Displays the IP Security Maintenance menu. This menu is reserved for Technical Support Personnel.
`gea` Displays the GEA Maintenance menu. GEA maintenance commands are reserved for Technical Support Personnel.

/maint/dcbx

DCBX Maintenance

```
[DCBX Debug  Menu]
     featcfg  - Display Feature Configuration
     ctrlst   - Display Control State Machine state
     featst   - Display Feature State Machine state
     txlist   - Display DCBX TX TLV list
     rxlist   - Display DCBX RX TLV list
     vniccur  - Display current VNIC cfg
     vnicpeer - Display if the peers on port support VNIC
```

Table 397. DCBX Maintenance Options

Command Syntax and Usage
`featcfg` Displays DCBX feature information.
`ctrlst` *<port alias or number>* Displays information about the Control state machine for the selected port.
`featst` *<port alias or number>* Displays information about the Feature state machine for the selected port.
`txlist` Displays the Type-Length-Value (TLV) list transmitted in the DCBX TLV.
`rxlist` Displays the Type-Length-Value (TLV) list received in the DCBX TLV.
`vniccur` *<port alias or number>* Displays the current vNIC configuration parameters for the selected port.
`vnicpeer` Displays a list of peers that support vNIC functionality.

/maint/lldp

LLDP Cache Manipulation Menu

```
[LLDP Menu]
     port     - Show LLDP port information
     rx       - Show LLDP receive state machine information
     tx       - Show LLDP transmit state machine information
     remodev  - Show LLDP remote devices information
     dump     - Show all LLDP information
     clear    - Clear LLDP remote devices information
```

Table 398 describes the LLDP cache manipulation commands.

Table 398. LLDP Cache Manipulation Options (/maint/lldp)

Command Syntax and Usage
`port` *<port alias or number>* Displays Link Layer Discovery Protocol (LLDP) port information.
`rx` Displays information about the LLDP receive state machine.
`tx` Displays information about the LLDP transmit state machine.
`remodev` [*<1-256>*|`detail`] Displays information received from LLDP -capable devices. To view information about a specific device, enter the index number of that device. To view detailed information about all devices, use the `detail` option.
`dump` Displays all LLDP information.
`clear` Clears the LLDP cache.

/maint/arp

ARP Cache Maintenance Menu

```
[Address Resolution Protocol Menu]
     find     - Show a single ARP entry by IP address
     port     - Show ARP entries on a single port
     vlan     - Show ARP entries on a single VLAN
     addr     - Show ARP entries for switch's interfaces
     dump     - Show all ARP entries
     clear    - Clear ARP cache
```

Table 399 describes the ARP cache maintenance menu options.

Table 399. ARP Maintenance Menu Options (/maint/arp)

Command Syntax and Usage
`find` *<IP address (such as, 192.4.17.101)>* Shows a single ARP entry by IP address.
`port` *<port alias or number>* Shows ARP entries on a single port.
`vlan` *<VLAN number>* Shows ARP entries on a single VLAN.
`addr` Shows the list of IP addresses which the switch will respond to for ARP requests.
`dump` Shows all ARP entries.
`clear` Clears the entire ARP list from switch memory.

Note: To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (`find`, `port`, `vlan`, `dump`), you can also refer to “ARP Information” on page 58.

/maint/route

IPv4 Route Manipulation Menu

```
[IP Routing Menu]
     find     - Show a single route by destination IP address
     gw       - Show routes to a single gateway
     type     - Show routes of a single type
     tag      - Show routes of a single tag
     if       - Show routes on a single interface
     dump     - Show all routes
     clear    - Clear route table
     nh       - Nexhop list
     re       - Route entry Nexhop list
```

Table 400 describes the IPv4 route manipulation menu options.

Table 400. IPv4 Route Manipulation Menu Options (/maint/route)

Command Syntax and Usage
`find` *<IP address (such as, 192.4.17.101)>* Shows a single route by destination IP address.
`gw` *<default gateway address (such as, 192.4.17.44)>* Shows routes to a default gateway.
`type indirect|direct|local|broadcast|martian|multicast` Shows routes of a single type. For a description of IP routing types, see Table 38 on page 57.
`tag fixed|static|addr|rip|ospf|bgp|broadcast|martian|multicast` Shows routes of a single tag. For a description of IP routing tags, see Table 39 on page 58.
`if` *<interface number>* Shows routes on a single interface.
`dump` Shows all routes.
`clear` Clears the route table from switch memory.
`nh` Displays the Next Hop list.
`re` Displays the route entry Next Hop list

Note: To display all routes, you can also refer to “IPv4 Routing Information” on page 56.

/maint/igmp

IGMP Maintenance Menu

```
[IGMP Multicast Group Menu]
     group    - Multicast Group Menu
     mrouter  - IGMP Multicast Router Port Menu
     clear    - Clear group and mrouter tables
```

Table 401 describes the IGMP Maintenance commands.

Table 401. IGMP Maintenance Menu Options (/maint/igmp)

Command Syntax and Usage
`group` Displays the Multicast Group menu. To view menu options, see page 472.
`mrouter` Displays the Multicast Router Port menu. To view menu options, see page 472.
`clear` Clears the IGMP group table and Mrouter tables.

/maint/igmp/group

IGMP Group Maintenance Menu

```
[IGMP Multicast Group Menu]
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     detail   - Show detail of a single group by IP address
     dump     - Show all groups
     clear    - Clear group tables
```

Table 402 describes the IGMP Maintenance commands.

Table 402. IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage
`find` *<IP address>* Displays a single IGMP multicast group by its IP address.
`vlan` *<VLAN number>* Displays all IGMP multicast groups on a single VLAN.
`port` *<port number or alias>* Displays all IGMP multicast groups on a single port.
`trunk` *<trunk number>* Displays all IGMP multicast groups on a single trunk group.

Table 402. IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage
`detail` *<IP address>* Displays detailed information about a single IGMP multicast group.
`dump` Displays information for all multicast groups.
`clear` Clears the IGMP group tables.

/maint/igmp/mrouter
IGMP Multicast Routers Maintenance Menu

```
[IGMP Multicast Routers Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all multicast router ports
     clear    - Clear multicast router port table
```

Table 403 describes the IGMP multicast router (Mrouter) maintenance commands.

Table 403. IGMP Mrouter Maintenance Menu Options (/maint/igmp/mrouter)

Command Syntax and Usage
`vlan` *<VLAN number>* Shows all IGMP multicast router ports on a single VLAN.
`dump` Shows all multicast router ports.
`clear` Clears the IGMP Multicast Router port table.

/maint/mld

MLD Multicast Group Manipulation

```
[MLD Multicast Group Menu]
     groups   - Show all groups
     find     - Show a single group by IP group address
     vlan     - Show groups on a single vlan
     port     - Show groups on a single port
     trunk    - Show groups on a single trunk
     if       - Show interface(s) mld information
     mrclear  - Clear dynamic MLD mrouter group tables
     grclear  - Clear dynamic MLD registerd group tables
     clear    - Clear dynamic MLD group tables
```

Table 406 describes the Multicast Listener Discovery (MLD) maintenance options.

Table 404. MLD Maintenance (/maint/mld)

Command Syntax and Usage
`groups` Shows all MLD groups.
`find` *<IPv6 address>* Shows a MLD single group by IP group address.
`vlan` *<VLAN number>* Shows MLD groups on a single VLAN.
`port` *<port alias or number>* Shows MLD groups on a single port.
`trunk` *<trunk group number>* Shows MLD groups on a single trunk.
`if` *<interface number>* Shows MLD groups on the specified interface.
`mrclear` Clears all dynamic MLD multicast router group tables.
`grclear` Clears all dynamic MLD registered group tables.
`clear` Clears all dynamic MLD group tables.

/maint/lacp

LACP Maintenance

```
[Link Aggregation Control Protocol Menu]
     txmarker - Send an LACP Marker packet (only for debug purpose)
```

Table 406 describes the Link Aggregation Control Protocol manipulation options.

Table 405. Link Aggregation Control Protocol Manipulation

Command Syntax and Usage
`txmarker` *<port number>* Send an LACP Marker packet (for debugging only).

/maint/nbrcache

IPv6 Neighbor Discovery Cache Manipulation

```
[Neighbor Cache Manipulation Menu]
     find     - Show a single NBR Cache entry by IP address
     port     - Show NBR Cache entries on a single port
     vlan     - Show NBR Cache entries on a single VLAN
     dump     - Show all NBR Cache entries
     clear    - Clear neighbor cache
```

Table 406 describes the IPv6 Neighbor Discovery cache manipulation options.

Table 406. IPv6 Neighbor Discovery Cache Manipulation (/maint/nbrcache)

Command Syntax and Usage
`find` *<IPv6 address>* Shows a single IPv6 Neighbor Discovery cache entry by IP address.
`port` *<port alias or number>* Shows IPv6 Neighbor Discovery cache entries on a single port.
`vlan` *<VLAN number>* Shows IPv6 Neighbor Discovery cache entries on a single VLAN.
`dump` Shows all IPv6 Neighbor Discovery cache entries.
`clear` Clears all IPv6 Neighbor Discovery cache entries from switch memory.

/maint/route6
IPv6 Route Manipulation Menu

```
[IP6 Routing Menu]
     dump     - Show all routes
     clear    - Clear route table
```

Table 407 describes the IPv6 Route maintenance options.

Table 407. IPv6 Route Manipulation (/maint/route6)

Command Syntax and Usage
`dump` Shows all IPv6 routes.
`clear` Clears all IPv6 routes from switch memory.

/maint/uudmp
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 `uudmp` command. This will ensure that you do not lose any information. Once entered, the `uudmp` command will cause approximately 23,300 lines of data to be displayed on your screen and copied into the file.

Using the `uudmp` 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 477.

To access dump information, at the `Maintenance#` prompt, enter:

```
Maintenance# uudmp
```

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.
```

/maint/ptdmp <*FTP/TFTP/SFTP server*> <*filename*> [-mgt|-extm|-data]

FTP/TFTP/SFTP System Dump Put

Use this command to put (save) the system dump to a FTP/TFTP/SFTP server.

Note: If the FTP/TFTP/SFTP server is running SunOS or the Solaris operating system, the specified ptdmp file must exist *prior* to executing the ptdmp 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 dump data.

To save dump information via FTP/TFTP/SFTP, at the Maintenance# prompt, enter:

```
Maintenance# ptdmp <FTP/TFTP/SFTP server> <filename> [-mgt|-extm|-data]
```

Where *server* is the FTP/TFTP/SFTP server IP address or hostname, and *filename* is the target dump file. The default port option is -mgt.

/maint/cldmp

Clearing Dump Information

To clear dump information from flash memory, at the Maintenance# prompt, enter:

```
Maintenance# cldmp
```

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, 2012. Use /maint/uudmp to
      extract the dump for analysis and /maint/cldmp to
      clear the FLASH region. The region must be cleared
      before another dump can be saved.
```

Appendix A. System Log Messages

The CN4093 10Gb Converged Scalable Switch (CN4093) uses the following syntax when outputting system log (syslog) messages:

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

The following parameters are used:

- *<Timestamp>*

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

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

  For example: `Aug 19 14:20:30`

- <*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	Fast Forward port <*port*> active, putting port into forwarding state
STP	New preferred Fast Uplink port <*port*> active for STG <*STG*>, {restarting | canceling} timer
STP	own BPDU received from port <*port*>
STP	Port <*port*>, putting port into blocking state
STP	Preferred STG <*STG*> Fast Uplink port has gone down. Putting secondary Fast Uplink port <*port*> into forwarding
STP	Setting STG <*STG*> Fast Uplink primary port <*port*> forwarding and backup port <*port*> blocking

Thread	LOG_ALERT Message (continued)
STP	STG <*STG*> preferred Fast Uplink port <*port*> active. Waiting <*seconds*> seconds before switching from port <*port*>
STP	STG <*STG*>, new root bridge
STP	STG <*STG*>, topology change detected
STP	STG <*STG*> root port <*port*> has gone down. Putting backup Fast Uplink port <*port*> into forwarding
SYSTEM	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <key>
VRRP	Received <x> virtual routers instead of <y>
VRRP	received errored advertisement from <*IP address*>
VRRP	received incorrect addresses from <*IP address*>
VRRP	received incorrect advertisement interval <interval> from <*IP address*>
VRRP	received incorrect VRRP authentication type from <*IP address*>
VRRP	received incorrect VRRP password from <*IP address*>
VRRP	VRRP : received incorrect IP addresses list from <*IP address*>

LOG_CRIT

Thread	LOG_CRIT Message
SSH	can't allocate memory in load_MP_INT()
SSH	currently not enough resource for loading RSA {private | public key}
SYSTEM	System memory is at <*n*> percent

LOG_ERR

Thread	LOG_ERR Message
CFG	Configuration file is EMPTY
CFG	Configuration is too large
CFG	Default VLAN cannot be a private-VLAN.
CFG	Error writing active config to FLASH! Configuration is too large
CFG	Error writing active config to FLASH! Unknown error
CFG	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
DCBX	Duplicate DCBX Application Protocol Sub-TLV detected on port *<port>*
DCBX	Duplicate DCBX Control Sub-TLV detected on port *<port>*
DCBX	Duplicate DCBX PFC Sub-TLV detected on port *<port>*
DCBX	Duplicate DCBX PG Sub-TLV detected on port *<port>*
DCBX	Duplicate DCBX VNIC Sub-TLV detected on port *<port>*
DCBX	Multiple peers detected on port *<port>*
ETS	The internal COS7 is used for stack communication. The ETS priority group 7 is not available.
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
PFC	PFC can be enabled on 2 priorities only: priority 3 and one other priority.
STP	Cannot set "{Hello Time | Max Age | Forward Delay | Aging}" (Switch is in MSTP mode)

Thread	LOG_ERR Message (continued)
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
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting

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

Thread	LOG_INFO Message (continued)
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...
DCBX	Detected DCBX peer on port *<port>*
DCBX	Feature "{DCBX | ETS | PFC | App Proto | VNIC | ETS}" not supported by peer on port *<port>*
DCBX	LLDP [TX &] RX are disabled on port *<port>*
DCBX	LLDP TX is disabled on port *<port>*
DCBX	Not able to detect DCBX peer on port *<port>*
DCBX	Peer on port port stopped responding to DCBX message
FCOE	Failed to create FCOE vlan *<VLAN>*
FCOE	FCF *<MAC address>* has been removed.
FCOE	FCF *<MAC address>* is now operational.
FCOE	FCOE connection between VN_PORT *<MAC address>* and FCF *<MAC address>* {has been established | is down}.
FCOE	FCOE vlan *<VLAN>* created.
FCOE	Port *<port>* has been added to the FCOE vlan *<VLAN>*.
FCOE	VN_PORT *<MAC address>* has been reassigned, the old connection will be deleted.
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
IP	default gateway *<IP address>* {disabled | enabled | operational}

Thread	LOG_NOTICE Message (continued)
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
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	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>*}

Thread	LOG_NOTICE Message (continued)
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}
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>*

Thread	LOG_NOTICE Message (continued)
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 by BPDU Guard
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
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*>.
ETS	ETS prohibits a PG comprising of PFC and non-PFC traffic. Mixing in the same PG different PFC settings may affect the switch functionality.
HOTLINKS	"Error" is set to "Standby | Active"
HOTLINKS	"Learning" is set to "Standby | Active"
HOTLINKS	"None" is set to "Standby | Active"
HOTLINKS	"Side Max" is set to "Standby | Active"
HOTLINKS	has no "{Side Max | None | Learning | Error}" interface
NTP	cannot contact [primary | secondary] NTP server <*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. SNMP Agent

SNMP Overview

The IBM Networking OS SNMP agent supports SNMP version 3. Security is provided through SNMP community strings. The default community strings are "`public`" for `SNMP GET` operation and "`private`" for `SNMP SET` operation. The community string can be modified only through the Command Line Interface (CLI). IBM is registered as Vendor 20301.

Detailed SNMP MIBs and trap definitions of the IBM Networking OS SNMP agent are contained in the following IBM Networking OS enterprise MIB document:

```
ScSE-10G-L2L3.mib
```

The IBM Networking OS SNMP agent supports the following standard MIBs:

- `rfc1213.mib`
- `rfc1215.mib`
- `rfc1493.mib`
- `rfc1573.mib`
- `rfc1643.mib`
- `rfc1757.mib`
- `rfc1907.mib`
- `rfc2037.mib`
- `rfc2571.mib`
- `rfc2572.mib`
- `rfc2573.mib`
- `rfc2574.mib`
- `rfc2575.mib`
- `rfc2576.mib`
- `ieee8021ab.mib`
- `dot1x.mib`
- `rfc1657.mib`
- `rfc1850.mib`

The IBM Networking OS SNMP agent supports the following generic traps as defined in RFC 1215:

- ColdStart
- WarmStart
- LinkDown
- LinkUp
- AuthenticationFailure

The SNMP agent also supports two Spanning Tree traps as defined in RFC 1493:

- NewRoot
- TopologyChange

The following are the enterprise SNMP traps supported in IBM Networking OS:

Table 408. IBM Networking OS-Supported Enterprise SNMP Traps

Trap Name	Description
altSwDefGwUp	Signifies that the default gateway is alive.
altSwDefGwDown	Signifies that the default gateway is down.
altSwDefGwInService	Signifies that the default gateway is up and in service
altSwDefGwNotInService	Signifies that the default gateway is alive but not in service
altSwVrrpNewMaster	Indicates that the sending agent has transitioned to 'Master' state.
altSwVrrpNewBackup	Indicates that the sending agent has transitioned to 'Backup' state.
altSwVrrpAuthFailure	Signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional.
altSwLoginFailure	Signifies that someone failed to enter a valid username/password combination.
altSwTempExceedThreshold	Signifies that the switch temperature has exceeded maximum safety limits.
altSwTempReturnThreshold	Signifies that the switch temperature has returned below maximum safety limits.
altSwStgNewRoot	Signifies that the bridge has become the new root of the STG.
altSwStgTopologyChanged	Signifies that there was a STG topology change.
altSwStgBlockingState	An altSwStgBlockingState trap is sent when port state is changed in blocking state.
altSwCistNewRoot	Signifies that the bridge has become the new root of the CIST.
altSwCistTopologyChanged	Signifies that there was a CIST topology change.
altSwHotlinksMasterUp	Signifies that the Master interface is active.
altSwHotlinksMasterDn	Signifies that the Master interface is not active.
altSwHotlinksBackupUp	Signifies that the Backup interface is active.
altSwHotlinksBackupDn	Signifies that the Backup interface is not active.
altSwHotlinksNone	Signifies that there are no active interfaces.

Switch Images and Configuration Files

This section describes how to use MIB calls to work with switch images and configuration files. You can use a standard SNMP tool to perform the actions, using the MIBs listed in Table 409.

Table 409 lists the MIBS used to perform operations associated with the Switch Image and Configuration files.

Table 409. MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTransferServer	1.3.6.1.4.1.20301.2.5.1.1.7.1.0
agTransferImage	1.3.6.1.4.1.20301.2.5.1.1.7.2.0
agTransferImageFileName	1.3.6.1.4.1.20301.2.5.1.1.7.3.0
agTransferCfgFileName	1.3.6.1.4.1.20301.2.5.1.1.7.4.0
agTransferDumpFileName	1.3.6.1.4.1.20301.2.5.1.1.7.5.0
agTransferAction	1.3.6.1.4.1.20301.2.5.1.1.7.6.0
agTransferLastActionStatus	1.3.6.1.4.1.20301.2.5.1.1.7.7.0
agTransferUserName	1.3.6.1.4.1.20301.2.5.1.1.7.9.0
agTransferPassword	1.3.6.1.4.1.20301.2.5.1.1.7.10.0
agTransferTSDumpFileName	1.3.6.1.4.1.20301.2.5.1.1.7.11.0

The following SNMP actions can be performed using the MIBs listed in Table 409.

- Load a new Switch image (boot or running) from a FTP/TFTP server
- Load a previously saved switch configuration from a FTP/TFTP server
- Save the switch configuration to a FTP/TFTP server
- Save a switch dump to a FTP/TFTP server

Loading a New Switch Image

To load a new switch image with the name "`MyNewImage-1.img`" into `image2`, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch image resides:

   ```
   Set agTransferServer.0 "192.168.10.10"
   ```

2. Set the area where the new image will be loaded:

   ```
   Set agTransferImage.0 "image2"
   ```

3. Set the name of the image:

   ```
   Set agTransferImageFileName.0 "MyNewImage-1.img"
   ```

4. If you are using an FTP server, enter a username:

   ```
   Set agTransferUserName.0 "MyName"
   ```

5. If you are using an FTP server, enter a password:

   ```
   Set agTransferPassword.0 "MyPassword"
   ```

6. Initiate the transfer. To transfer a switch image, enter 2 (gtimg):

   ```
   Set agTransferAction.0 "2"
   ```

Loading a Saved Switch Configuration

To load a saved switch configuration with the name “MyRunningConfig.cfg” into the switch, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch Configuration File resides:

   ```
   Set agTransferServer.0 "192.168.10.10"
   ```

2. Set the name of the configuration file:

   ```
   Set agTransferCfgFileName.0 "MyRunningConfig.cfg"
   ```

3. If you are using an FTP server, enter a username:

   ```
   Set agTransferUserName.0 "MyName"
   ```

4. If you are using an FTP server, enter a password:

   ```
   Set agTransferPassword.0 "MyPassword"
   ```

5. Initiate the transfer. To restore a running configuration, enter 3:

   ```
   Set agTransferAction.0 "3"
   ```

Saving the Switch Configuration

To save the switch configuration to a FTP/TFTP server follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the configuration file is saved:

   ```
   Set agTransferServer.0 "192.168.10.10"
   ```

2. Set the name of the configuration file:

   ```
   Set agTransferCfgFileName.0 "MyRunningConfig.cfg"
   ```

3. If you are using an FTP server, enter a username:

   ```
   Set agTransferUserName.0 "MyName"
   ```

4. If you are using an FTP server, enter a password:

   ```
   Set agTransferPassword.0 "MyPassword"
   ```

5. Initiate the transfer. To save a running configuration file, enter 4:

   ```
   Set agTransferAction.0 "4"
   ```

Saving a Switch Dump

To save a switch dump to a FTP/TFTP server, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the configuration will be saved:

   ```
   Set agTransferServer.0 "192.168.10.10"
   ```

2. Set the name of dump file:

   ```
   Set agTransferDumpFileName.0 "MyDumpFile.dmp"
   ```

3. If you are using an FTP server, enter a username:

   ```
   Set agTransferUserName.0 "MyName"
   ```

4. If you are using an FTP server, enter a password:

   ```
   Set agTransferPassword.0 "MyPassword"
   ```

5. Initiate the transfer. To save a dump file, enter 5:

   ```
   Set agTransferAction.0 "5"
   ```

Appendix C. Appendix D. 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 Flex System 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, Flex System 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

Appendix E. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document. Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A0153039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

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

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis:

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

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

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.”

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)”. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
E-mail: tjahn@de.ibm.com

Generelle Informationen:

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

Japan VCCI Class A statement

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

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

Korea Communications Commission (KCC) statement

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

Russia Electromagnetic Interference (EMI) Class A statement

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

People’s Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

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

Taiwan Class A compliance statement

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

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Part Number: 00D2327

Printed in USA

(IP) P/N: 00D2327