IBM BladeCenter 1/10Gb Uplink Ethernet Switch Module

Menu-Based CLI Reference

IBM BladeCenter 1/10Gb Uplink Ethernet Switch Module

Menu-Based CLI Reference

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 (September 2012)

Contents

Preface

The *IBM N/OS™ 7.4 Menu-Based CLI for the 1/10Gb Uplink ESM for IBM BladeCenter® Command Reference* describes how to configure and use the IBM N/OS 7.4 software with your 1/10Gb Uplink ESM (GbESM) for IBM BladeCenter.

For documentation on installing the switches physically, see the *Installation Guide* for your GbESM. For details about configuration and operation of your GbESM, see the *IBM N/OS 7.4 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 3, "Menu Basics," provides an overview of the menu system, including a menu map, global commands, and menu shortcuts.

Chapter 4, "The Information Menu," shows how to view switch configuration parameters.

Chapter 5, "The Statistics Menu," shows how to view switch performance statistics.

Chapter 6, "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 7, "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 8, "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 9, "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, "IBM N/OS System Log Messages," shows a listing of syslog messages.

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

Appendix C, "Getting help and technical assistance," describes how to get help, service, or technical assistance or more information about IBM products.

"Index" includes pointers to the description of the key words used throughout the book.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1. Typographic Conventions

Typeface or Symbol	Meaning
`plain fixed-width text`	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|dip]`
	
	you enter:
	`/cfg/l3/route/ecmphash sip`
	
	or
	`/cfg/l3/route/ecmphash dip`
	
	or
	`/cfg/l3/route/ecmphash sip dip`

Chapter 1. The Command Line Interface

Your 1/10Gb Uplink ESM (GbESM) 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 N/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 N/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 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 GbESM

Management Module Setup

The BladeCenter GbESM is an integral subsystem within the overall BladeCenter system. The BladeCenter chassis includes a management module as the central element for overall chassis management and control.

You can use the management module to configure and manage the GbESM. The GbESM communicates with the management module(s) through its internal port 15 (MGT1) and port 16 (MGT2), which you can access through the 100 Mbps Ethernet port on each management module. The factory default settings permit management and control access to the switch module through *only* the management module or the built-in serial port. You can use the external Ethernet ports (EXT*x*) on the switch module for management and control of the switch, by selecting this mode as an option through the management module configuration utility program (see the applicable *BladeCenter Installation and User's Guide* publications for more information).

Note: Support for each management module is provided by a separate management port (MGT1 and MGT2). One port is active, and the other is used as a backup.

Factory-Default vs. MM-Assigned IP Addresses

Each GbESM must be assigned its own Internet Protocol address, which is used for communication with an SNMP network manager or other Transmission Control Protocol/Internet Protocol (TCP/IP) applications (for example, BootP or TFTP). The factory-default IP address is 10.90.90.9*x*, where x corresponds to the number of the bay into which the GbESM is installed. For additional information, see the *Installation Guide*). The management module assigns an IP address of 192.168.70.1*xx*, where *xx* corresponds to the number of the bay into which each GbESM is installed, as shown in the following table:

Table 2. GbESM IP addresses, based on switch-module bay numbers

Bay number	Factory-default IP address	IP address assigned by MM
Bay 1	10.90.90.91	192.168.70.127
Bay 2	10.90.90.92	192.168.70.128
Bay 3	10.90.90.94	192.168.70.129
Bay 4	10.90.90.97	192.168.70.130

Note: Switch Modules installed in Bay 1 and Bay 2 connect to server NICs 1 and 2, respectively. However, Windows operating systems show that Switch Modules installed in Bay 3 and Bay 4 connect to server NICs 4 and 3, respectively.

Default Gateway

The default Gateway IP address determines where packets with a destination address outside the current subnet are sent. Usually, the default Gateway is a router or host acting as an IP gateway to handle connections to other subnets of other TCP/IP networks. If you want to access the GbESM from outside your local network, use the management module to assign a default Gateway address to the GbESM. Choose **I/O Module Tasks > Configuration** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

Configuring Management Module for Switch Access

Complete the following initial configuration steps:

1. Connect the Ethernet port of the management module to a 10/100 Mbps network (with access to a management station) or directly to a management station.
2. Access and log on to the management module, as described in the *BladeCenter Management Module User's Guide*. The management module provides the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User's Guide* publications for more information).
3. Select Configuration on the I/O Module Tasks menu on the left side of the BladeCenter Management Module window. See Figure 1.

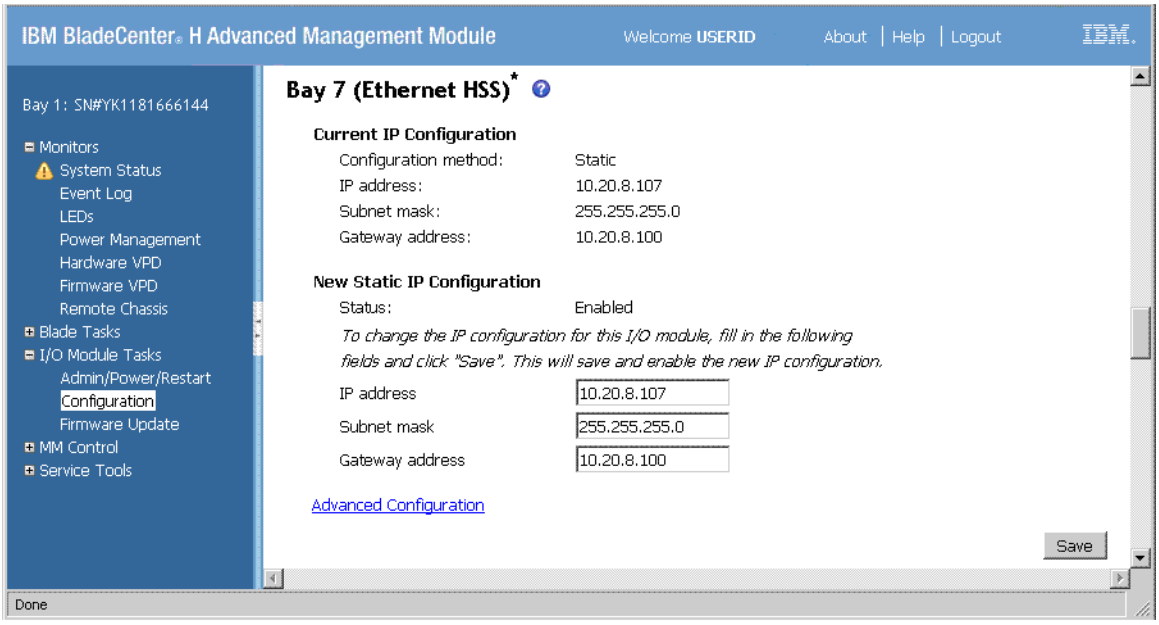


Figure 1. Switch Management on the BladeCenter Management Module

4. You can use the default IP addresses provided by the management module, or you can assign a new IP address to the switch module through the management module. You can assign this IP address through one of the following methods:
   - Manually through the BladeCenter management module
   - Automatically through the IBM Director Configuration Wizard

Note: If you change the IP address of the GbESM, make sure that the switch module and the management module both reside on the same subnet.

5. Enable the following features in the management module:
   – External Ports (**I/O Module Tasks > Admin/Power/Restart > Advanced Setup**)
   – External management over all ports **(Configuration > Advanced Configuration)**

     This setting is required if you want to access the management network through the external data ports (EXTx) on the GbESM.

The default value is `Disabled` for both features. If these features are not already enabled, change the value to `Enabled`, then `Save`.

Note: In **Advanced Configuration > Advanced Setup**, enable "Preserve new IP configuration on all switch resets" to retain the switch's IP interface when you restore factory defaults. This setting preserves the management port's IP address in the management module's memory so you maintain connectivity to the management module after a reset.

You can now start a telnet session, Browser-Based Interface (Web) session, a Secure Shell session, or a secure HTTPS session to the GbESM.

Connecting to the Switch via Telnet

Configuring the Switch for Telnet Access

Use the management module to access the GbESM through Telnet. Choose **I/O Module Tasks > Configuration** from the navigation pane on the left. Select a bay number and click **Advanced Configuration > Start Telnet/Web Session > Start Telnet Session**. A Telnet window opens a connection to the Switch Module (requires Java 1.4 Plug-in).

Once that you have configured the GbESM with an IP address and gateway, you can access the switch from any workstation connected to the management network. Telnet access provides the same options for user and administrator access as those available through the management module, minus certain Telnet and management commands.

To establish a Telnet connection with the switch, run the Telnet program on your workstation and issue the Telnet command, followed by the switch IP address:

```
telnet <switch IP address>
```

The command line interface recognizes both CR and LF as end-of-line markers. Consequently, Telnet clients using CR+LF end-of-line markers will produce double line breaks, impairing interaction with the command line interface. In such instances, adjust your Telnet client to use either CR or LF.

Using Telnet to Access the Switch

Once the IP parameters on the GbESM are configured, you can access the CLI using a Telnet connection. From the management module, you can establish a Telnet connection with the switch.

You will then be prompted to enter a password as explained on page 6.

Connecting to the Switch via SSH

Although a remote network administrator can manage the configuration of a GbESM via Telnet, this method does not provide a secure connection. The SSH (Secure Shell) protocol enables you to securely log into another device over a network to execute commands remotely. As a secure alternative to using Telnet to manage switch configuration, SSH ensures that all data sent over the network is encrypted and secure.

The switch can do only one session of key/cipher generation at a time. Thus, a SSH/SCP client will not be able to login if the switch is doing key generation at that time. Similarly, the system will fail to do the key generation if a SSH/SCP client is logging in at that time.

The supported SSH encryption and authentication methods are listed below.

- Server Host Authentication: Client RSA-authenticates the switch in the beginning of every connection.
- Key Exchange: RSA
- Encryption: 3DES-CBC, DES
- User Authentication: Local password authentication, RADIUS, TACACS+

The following SSH clients have been tested:

- OpenSSH_5.1p1 Debian-3ubuntu1
- SecureCRT 5.0 (Van Dyke Technologies, Inc.)
- Putty beta 0.60

Note: The IBM N/OS implementation of SSH supports both versions 1.5 and 2.0 and supports SSH client version 1.5 - 2.x.

Using SSH to Access the Switch

Once the IP parameters are configured and the SSH service is enabled on the GbESM (it is disabled by default), you can access the command line interface using an SSH connection.

To establish an SSH connection with the switch, run the SSH program on your workstation by issuing the SSH command, followed by the switch IP address:

```
>> # ssh <switch IP address>
```

If SecurID authentication is required, use the following command:

```
>> # ssh -1 ace <switch IP address>
```

You will then be prompted to enter your user name and password.

Accessing the Switch

To enable better switch management and user accountability, three levels or *classes* of user access have been implemented on the GbESM. 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 GbESM. 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 GbESM. 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 GbESM. 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 14.

Table 3. User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	The Operator 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 GbESM, 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 19.”

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. For information on changing this parameter, see “System Configuration Menu” on page 207.

Chapter 2. First-Time Configuration

To help with the initial process of configuring your switch, the IBM N/OS software includes a Setup utility. The Setup utility prompts you step-by-step to enter all the necessary information for basic configuration of the switch. This chapter describes how to use the Setup utility and how to change system passwords. Before you run Setup, you must first connect to the switch (see “Connecting to the Switch” on page 2).

Using the Setup Utility

Whenever you log in as the system administrator under the factory default configuration, you are asked whether you wish to run the Setup utility. Setup can also be activated manually from the command line interface any time after login.

Information Needed for Setup

Setup requests the following information:

- Basic system information
  - Date & time
  - Whether to use Spanning Tree Group or not
- Optional configuration for each port
  - Speed, duplex, flow control, and negotiation mode (as appropriate)
  - Whether to use VLAN tagging or not (as appropriate)
- Optional configuration for each VLAN
  - Name of VLAN
  - Which ports are included in the VLAN
- Optional configuration of IP parameters
  - IP address, subnet mask, and VLAN for each IP interface
  - IP addresses for default gateway
  - Destination, subnet mask, and gateway IP address for each IP static route
  - Whether IP forwarding is enabled or not
  - Whether the RIP supply is enabled or not

Starting Setup When You Log In

The Setup prompt appears automatically whenever you login as the system administrator under the factory default settings.

1. Connect to the switch.

   After connecting, the login prompt will appear as shown.

```
Enter Password:
```

2. Enter `admin` as the default administrator password.

   If the factory default configuration is detected, the system prompts:

```
1/10Gb Uplink Ethernet Switch Module
18:44:05 Wed Jan 3, 2010

The switch is booted with factory default configuration.
To ease the configuration of the switch, a "Set Up" facility which
will prompt you with those configuration items that are essential to the
operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n]:
```

Note: If the default `admin` login is unsuccessful, or if the administrator Main Menu appears instead, the system configuration has probably been changed from the factory default settings. If you are certain that you need to return the switch to its factory default settings, see "Selecting a Configuration Block" on page 474.

3. Enter `y` to begin the initial configuration of the switch, or n to bypass the Setup facility.

Stopping and Restarting Setup Manually

Follow these instructions to manually stop and restart setup.

Stopping Setup

To abort the Setup utility, press <Ctrl-C> during any Setup question. When you abort Setup, the system will prompt:

```
Would you like to run from top again? [y/n]
```

Enter `n` to abort Setup, or `y` to restart the Setup program at the beginning.

Restarting Setup

You can restart the Setup utility manually at any time by entering the following command at the administrator prompt:

```
# /cfg/setup
```

After initial configuration is complete, it is recommended that you change the default passwords as shown in "Setting Passwords" on page 14.

Optional Setup for Telnet Support

Follow these instructions if you want to change telnet access.

Note: This step is optional. Perform this procedure only if you are planning on connecting to the GbESM through a remote Telnet connection.

1. Telnet is enabled by default. To change the setting, use the following command:

```
>> # /cfg/sys/access/tnet
```

2. Apply and save the configuration(s).

```
>> System# apply
>> System# save
```

Setting Passwords

It is recommended that you change the user and administrator passwords after initial configuration and as regularly as required under your network security policies.

To change the administrator password, you must login using the administrator password.

Note: If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

Changing the Default Administrator Password

The administrator has complete access to all menus, information, and configuration commands, including the ability to change both the user and administrator passwords.

The default password for the administrator account is `admin`. To change the default password, follow this procedure:

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# /cfg
```

The Configuration Menu is displayed.

```
[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
     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/TFTP server
     gtcfg    - Restore current configuration from FTP/TFTP server
     cur      - Display current configuration
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

The System Menu is displayed.

```
[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
     dlight   - Set system daylight savings
     idle     - Set timeout for idle CLI sessions
     linkscan - Set linkscan mode
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     dhcp     - Enable/disable use of DHCP on EXTM interface
     reminder - Enable/disable Reminders
     rstctrl  - Enable/disable System reset on panic
     pktlog   - Enable/disable CPU packet logging capability
     srvled   - Enable/disable Service Required LED
     cur      - Display current system-wide parameters
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

The System Access Menu is displayed.

```
[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
```

5. Select the administrator password.

```
System Access# user/admpw
```

6. Enter the current administrator password at the prompt:

```
Changing ADMINISTRATOR password; validation required...
Enter current administrator password:
```

Note: If you forget your administrator password, call your technical support representative for help using the password fix-up mode.

7. Enter the new administrator password at the prompt:

```
Enter new administrator password:
```

8. Enter the new administrator password, again, at the prompt:

```
Re-enter new administrator password:
```

9. Apply and save your change by entering the following commands:

```
System# apply
System# save
```

Changing the Default User Password

The user login has limited control of the switch. Through a user account, you can view switch information and statistics, but you can't make configuration changes.

The default password for the user account is `user`. This password can be changed from the user account. The administrator can change all passwords, as shown in the following procedure.

1. Connect to the switch and log in using the `admin` password.
2. From the Main Menu, use the following command to access the Configuration Menu:

```
Main# cfg
```

3. From the Configuration Menu, use the following command to select the System Menu:

```
>> Configuration# sys
```

4. From the System Menu, use the following command to select the System Access Menu:

```
>> System# access
```

5. Select the user password.

```
System# user/usrpw
```

6. Enter the current administrator password at the prompt.

   Only the administrator can change the user password. Entering the administrator password confirms your authority.

```
Changing USER password; validation required...
Enter current administrator password:
```

7. Enter the new user password at the prompt:

```
Enter new user password:
```

8. Enter the new user password, again, at the prompt:

```
Re-enter new user password:
```

9. Apply and save your changes:

```
System# apply
System# save
```

Chapter 3. Menu Basics

The IBM N/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 4. 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.
`lines` [<*0-300*>]	Sets the number of lines per screen displayed in the CLI for the current session. A value of 0 disables paging. By default, it is set to the corresponding `/cfg/sys/linevty` or `/cfg/sys/linecons` value effective at login (see page 207 for details). When used without a value, the current setting is displayed.
`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`.

Table 4. Description of Global Commands (continued)

Command	Action
`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 390).
`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.

Table 4. Description of Global Commands (continued)

Command	Action
`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 5. 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 4. 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
     stack    - Stacking 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
     dump     - Dump all information
```

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

Table 6. Information Menu Options (/info)

Command Syntax and Usage
`sys` Displays the System Information Menu. For details, see page 31.
`stack` Displays the Stacking Information Menu. For details, see page 45. **Note:** This option only appears if you have stacking turned on.
`l2` Displays the Layer 2 Information Menu. For details, see page 47.
`l3` Displays the Layer 3 Information Menu. For details, see page 68.
`qos` Displays the Quality of Service (QoS) Information Menu. For details, see page 102.
`acl` Displays the current configuration profile for each Access Control List (ACL) and ACL Group. For details, see page 106.

Table 6. Information Menu Options (/info)

Command Syntax and Usage
`rmon` Displays the Remote Monitoring (RMON) Information Menu. For details, see page 107.
`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 111.
`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 112.
`transcvr` Displays the status of the port transceiver module on each external port. For details, see page 113.
`virt` Displays the Virtualization information menu. For details, see page 114.
`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 7, with pointers to where detailed information can be found.

Table 7. System Menu Options (/info/sys)

Command Syntax and Usage
`errdis` Displays Error Disable and Recovery Information menu. To view the menu options, see page 32.
`snmpv3` Displays SNMPv3 Information Menu. To view the menu options, see page 33.
`chassis` Displays information about the BladeCenter chassis. For details, see page 42.
`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 43.
`log` Displays most recent syslog messages. For details, see page 44.
`user` Displays configured user names and their status. For details, see page 44.
`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 8. 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 9. 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 35.
`view` Displays information about view, sub-trees, mask and type of view. To view a sample, see page 35.
`access` Displays View-based Access Control information. To view a sample, see page 37.
`group` Displays information about the group that includes, the security model, user name, and group name. To view a sample, see page 38.
`comm` Displays information about the community table information. To view a sample, see page 38.
`taddr` Displays the Target Address table information. To view a sample, see page 39.
`tparam` Displays the Target parameters table information. To view a sample, see page 40.

Table 9. SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
`notify` Displays the Notify table information. To view a sample, see page 40.
`dump` Displays all the SNMPv3 information. To view a sample, see page 41.

/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 10. 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 N/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 11. 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 subsystem provides authorization services.

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

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

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

Table 12. SNMPv3 Access Table Information (/info/sys/snmpv3/access)

Field	Description
Group Name	Displays the name of group.
Prefix	Displays the prefix that is configured to match the values.
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`.
Match	Displays the match for the contextName. The options are: `exact` and `prefix`.
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 13. 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.
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 14. 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 15. 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.
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 16. 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 17. 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:
All active SNMPv3 groups are listed below:
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

BladeCenter Chassis Information

```
IBM BladeCenter Chassis Related Information:

    Switch Module Bay = 2
    Chassis Type      = BladeCenter H
    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 16:50:45 Wed Nov 16, 2011
Time zone: America/US/Pacific
Daylight Savings Time Status: Disabled

1/10Gb Uplink Ethernet Switch Module for IBM BladeCenter

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

MAC address: 00:11:58:ad:a3:00  Management IP Address (if 128): 10.90.90.97
Software Version 6.5.0 (FLASH image1), factory default configuration.


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

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

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

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 for which the administrator is being notified.

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

/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 lynn   , dis, cos user    , password valid, offline
Current strong password settings:
  strong password status: disabled
```

This command displays the status of the configured usernames.

/info/stack

Stacking Information Menu

```
[Stacking Menu]
     switch   - Show switch information
     link     - Show stack link information
     name     - Show stack name
     backup   - Show backup unit number
     vers     - Show switch firmware information
     path     - Show inter switch packet path map
     pushstat - Show config/image push status information
     dump     - Dump all stacking information
```

Note: The Stacking Information menu only appears if you have stacking turned on.

Table 18 lists the Stacking information menu options.

Table 18. Stacking Information Menu Options (/info/stack)

Command Syntax and Usage
`switch` Displays information about each switch in the stack, including: – Configured Switch Number (csnum) – Attached Switch Number (asnum) – MAC address – Stacking state
`link` Displays link information for each switch in the stack, listed by assigned switch number.
`name` Displays the name of the stack.
`backup` Displays the unit number of the backup switch.
`vers` Displays the firmware version number for the selected switch.
`path` Displays the Stacking packet path map that shows how the stack switches are connected.
`pushstat` Displays the status of the most recent firmware and configuration file push from the master to member switches.
`dump` Displays all stacking information.

/info/stack/switch

Stacking Switch Information

```
Stack name: MyStack
Local switch is the master.

Local switch:
   csnum             - 1
   MAC               - 00:25:03:1c:96:00
   Switch Type       - 9
   Switch Mode (cfg) - Master
   Priority          - 225
   Stack MAC         - 00:25:03:1c:96:1f

Master switch:
   csnum             - 1
   MAC               - 00:25:03:1c:96:00

Backup switch:
   csnum             - 2
   MAC               - 00:ef:61:79:00:00

Configured Switches:
-------------------------------------
csnum           MAC          asnum
-------------------------------------
 C1     00:25:03:1c:96:00    A1
 C2     00:ef:61:79:00:00    A2

Attached Switches in Stack:
---------------------------------------------
asnum           MAC          csnum  State
---------------------------------------------
 A1     00:25:03:1c:96:00     C1    IN_STACK
 A2     00:ef:61:79:00:00     C2    IN_STACK
```

Stack switch information includes the following:

- Stack name
- Details about the local switch from which the command was issued
- Configured switch number and MAC of the Stack Master and Stack Backup
- Configured switch numbers and their associated assigned switch numbers
- Attached switch numbers and their associated configured switch numbers

/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
     lldp     - LLDP Information Menu
     udld     - UDLD Information Menu
     oam      - OAM 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 19, with pointers to where detailed information can be found.

Table 19. Layer 2 Information Menu Options (/info/l2)

Command Syntax and Usage
`fdb` Displays the Forwarding Database Information Menu. For details, see page 50.
`lacp` Displays the Link Aggregation Control Protocol Menu. For details, see page 52.
`failovr` Displays the Layer 2 Failover Information menu. For details, see page 53.
`hotlink` Displays the Hot Links Information menu. For details, see page 54.
`lldp` Displays the LLDP Information menu. For details, see page 55.
`udld` Displays the Unidirectional Link Detection (UDLD) Information menu. For details, see page 57.
`oam` Displays the Operation, Administration, and Maintenance (OAM) Information menu. For details, see page 58.
`8021x` Displays the 802.1X Information Menu. For details, see page 59.

Table 19. Layer 2 Information Menu Options (/info/l2) (continued)

Command Syntax and Usage
`stg` Displays Spanning Tree information, including the status (on or off), Spanning Tree mode (STP/PVST+, RSTP, PVRST, 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 – Port Fast Forwarding state For details, see page 61.
`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 65.
`trunk` When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see page 67.

Table 19. Layer 2 Information Menu Options (/info/l2) (continued)

Command Syntax and Usage
`vlan` Displays VLAN configuration information, including: – VLAN Number – VLAN Name – Status – Port membership of the VLAN – VLAN management status For details, see page 67.
`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]
     mcast    - FDB multicast 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
     static   - Show FDB static unicast entries
     dump     - Show all non-multicast 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 16K MAC address entries on the MP per switch.

Table 20. FDB Information Menu Options (/info/l2/fdb)

Command Syntax and Usage
`mcast` Displays the FDB Multicast Menu. For details, see page 51.
`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.
`static` Displays all static unicast entries in the FDB.
`dump` Displays all non-multicast entries in the Forwarding Database. For more information, see page 51.

/info/l2/fdb/mcast

FDB Multicast Menu

```
[Multicast Menu]
     find     - Show a single FDB multicast entry by MAC address
     port     - Show FDB multicast entries on a single port
     vlan     - Show FDB multicast entries on a single VLAN
     dump     - Show all FDB multicast entries
```

The following table shows the forwarding database multicast options.

Table 21. FDB Multicast Menu Options (/info/l2/fdb/mcast)

Command Syntax and Usage
`find` *<MAC address>* [*<VLAN>*] Displays a single FDB multicast entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `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 multicast entries for a particular port.
`vlan` *<VLAN number (1-4094)>* Displays all FDB multicast entries on a single VLAN.
`dump` Displays all multicast entries in the Forwarding Database.

/info/l2/fdb/dump

Show All FDB Information

```
Mac address Aging Time: 300

Total number of FDB entries : 67
     MAC address     VLAN  Port     Trnk  State  Permanent
  -----------------  ----  -------  ----  -----  ---------
  00:00:01:00:00:01   100  EXT10           FWD
  00:00:5e:00:01:01     1  EXT11           FWD
  00:04:96:52:bc:97     1  EXT11           FWD
  00:05:73:a2:07:40     1  EXT11           FWD
  00:09:97:3e:21:c1     1  EXT11           FWD       P
...
```

When an address that is in the forwarding (`FWD`) state, this 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.

To clear the entire FDB, see “Forwarding Database Maintenance Menu” on page 484.

/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 22. 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 52.

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

```
port   mode     adminkey  operkey  selected   prio  aggr  trunk  status  minlinks
-------------------------------------------------------------------------------
INT1   active          1        1     yes    32768    17     19    up        1
INT2   active          2        2     yes    32768    17     19    up        1
INT3   off             3        3     no     32768    --     --    --        1
INT4   off             4        4     no     32768    --     --    --        1
...
```

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

- `port` Displays the port number or alias.
- `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).
- `minlinks` Displays the minimum number of active links this trunk group needs.

/info/l2/failovr
Layer 2 Failover Information Menu

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

Table 23 describes the Layer 2 Failover information options.

Table 23. 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
---------   -----------
 INT1       Operational
 INT2       Operational
 INT3       Operational
 INT4       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 these conditions are not true, the monitor port is considered to be failed.

A control port is considered to be operational if the monitor trigger state is `Up`. Even if a port's link status is `Down`, 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 24. 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 54.

/info/l2/hotlink/trigger
Hotlinks Trigger Information

```
Hot Links Info: Trigger

Current global Hot Links setting: OFF
bpdu disabled
sndfdb disabled
sndrate 40

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
- Send rate
- Status and configuration of each Hot Links trigger

/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
     instance - Show LLDP instance information
     dump     - Show all LLDP information
```

Table 25. LLDP Information Menu Options (/info/l2/lldp)

Command Syntax and Usage
`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 56.
`instance` Displays instance information received from LLDP -capable devices.
`dump` Displays all LLDP information.

/info/l2/lldp/remodev

LLDP Remote Device Information

```
LLDP Remote Devices Information

LocalPort | Index | Remote Chassis ID | RemotePort | Remote System Name
----------|-------|-------------------|------------|---------------------------
     MGT  | 210   | 00 16 ca ff 7e 00 | 15         | BNT Gb Ethernet Switch...
     EXT4 | 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 here, 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 1/10Gb Uplink Ethernet
Switch Module, IBM Networking OS: version 7.4.0,13 Boot image: version 7.4.0.13

        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 57.
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
```

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 58.
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/l2/8021x

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
-----  ------------  ------------  --------------  ---------- --------
*INT1  force-auth    unauthorized  initialize      initialize   none
*INT2  force-auth    unauthorized  initialize      initialize   none
 INT3  force-auth    unauthorized  initialize      initialize   none
*INT4  force-auth    unauthorized  initialize      initialize   none
 INT5  force-auth    unauthorized  initialize      initialize   none
*INT6  force-auth    unauthorized  initialize      initialize   none
*INT7  force-auth    unauthorized  initialize      initialize   none
*INT8  force-auth    unauthorized  initialize      initialize   none
*INT9  force-auth    unauthorized  initialize      initialize   none
 INT10 force-auth    unauthorized  initialize      initialize   none
*INT11 force-auth    unauthorized  initialize      initialize   none
*INT12 force-auth    unauthorized  initialize      initialize   none
 INT13 force-auth    unauthorized  initialize      initialize   none
*INT14 force-auth    unauthorized  initialize      initialize   none
 BR5A  force-auth    unauthorized  initialize      initialize   none
 BR5B  force-auth    unauthorized  initialize      initialize   none
 BR5C  force-auth    unauthorized  initialize      initialize   none
 BR5D  force-auth    unauthorized  initialize      initialize   none
 EXT5  force-auth    unauthorized  initialize      initialize   none
 EXT6  force-auth    unauthorized  initialize      initialize   none
*EXT7  force-auth    unauthorized  initialize      initialize   none
*EXT8  force-auth    unauthorized  initialize      initialize   none
*EXT9  force-auth    unauthorized  initialize      initialize   none
*EXT10 force-auth    unauthorized  initialize      initialize   none
*EXT11 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 BladeCenter unit that you are using and the firmware versions and options that are installed.

The following table describes the IEEE 802.1X parameters.

Table 28. 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.

Table 28. 802.1X Parameter Descriptions (/info/l2/8021x) (continued)

Parameter	Description
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 (STP/PVST+)
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
              65535      2      20      15     300

Port Priority Cost FastFwd    State      Designated Bridge    Des Port
---- -------- ---- -------   -------    -------------------   --------
INT1         0    0     n   FORWARDING  *
INT2         0    0     n   FORWARDING  *
INT3         0    0     n   FORWARDING  *
INT4         0    0     n   FORWARDING  *
INT5         0    0     n   FORWARDING  *
INT6         0    0     n   FORWARDING  *
INT7         0    0     n   FORWARDING  *
INT8         0    0     n   FORWARDING  *
INT9         0    0     n    DISABLED   *
INT10        0    0     n   FORWARDING  *
INT11        0    0     n   FORWARDING  *
INT12        0    0     n   FORWARDING  *
INT13        0    0     n   FORWARDING  *
INT14        0    0     n   FORWARDING  *
EXT1       128    2     n    DISABLED
EXT2       128    2     n    DISABLED
EXT3       128    2     n   FORWARDING    ffff-00:13:0a:4f:7d:d0    8011
EXT4       128    4!    n   FORWARDING    ffff-00:22:00:7d:71:00    8017
EXT5       128    2     n    DISABLED
...
* = STP turned off for this port.
! = Automatic path cost.
```

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

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). If IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), or Per VLAN Rapid Spanning Tree Protocol (PVRST) are turned on, see “RSTP/MSTP Information” on page 63.

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

Table 29. Spanning Tree 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 MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STG 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 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.
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.
FastFwd	The FastFwd shows whether the port is in Fast Forwarding mode or not, which permits the port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.
State	The state field shows the current state of the port. The state field can be `BLOCKING`, `LISTENING`, `LEARNING`, `FORWARDING`, or `DISABLED`.
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 identifier of the port on the Designated Bridge to which this port is connected.

/info/l2/stg

RSTP/MSTP 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
----- ---- --------- -----  ---- ---------------------- --------  -----
INT1     0         0  DSB *
INT2     0         0  DSB *
INT3     0         0  FWD *
INT4     0         0  DSB *
INT5     0         0  DSB *
INT6     0         0  DSB *
INT7     0         0  DSB *
INT8     0         0  DSB *
INT9     0         0  DSB *
INT10    0         0  DSB *
INT11    0         0  DSB *
INT12    0         0  DSB *
INT13    0         0  DSB *
INT14    0         0  DSB *
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
...
* = 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 BladeCenter unit 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 293), you can view RSTP/MSTP bridge information for the Spanning Tree Group and port-specific RSTP information.

The following table describes the STP parameters in RSTP or MSTP mode.

Table 30. RSTP/MSTP 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 MAC address of the root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.

Table 30. RSTP/MSTP 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.
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.
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
----- ---- --------- -----  ---- ---------------------- -------- ----- ----
 INT1     0         0  DSB *
 INT2     0         0  DSB *
 INT3     0         0  FWD *
 INT4     0         0  DSB *
 INT5     0         0  DSB *
 INT6     0         0  DSB *
 INT7     0         0  DSB *
 INT8     0         0  DSB *
 INT9     0         0  DSB *
 INT10    0         0  DSB *
 INT11    0         0  DSB *
 INT12    0         0  DSB *
 INT13    0         0  DSB *
 INT14    0         0  DSB *
 MGT1     0         0  FWD *
 MGT2     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 BladeCenter unit 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 31. 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.

Table 31. CIST Parameter Descriptions (continued)

Parameter	Description
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).
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  INT1-INT14 EXT1-EXT9
10    VLAN 10                         ena     dis  INT1
11    VLAN 11                         ena     dis  EXT3
30    VLAN 30                         ena     dis  EXT4
4095  Mgmt VLAN                       ena     ena  INT1-INT14 MGT1 MGT2
```

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

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

VLAN information includes:

- VLAN Number
- VLAN Name
- Status
- Management status of the VLAN
- 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
     dhcp     - DHCP Information Menu
     dump     - Dump all layer 3 information
```

The information provided by each menu option is briefly described in Table 32, with pointers to detailed information.

Table 32. 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 71.
`arp` Displays the Address Resolution Protocol (ARP) Information Menu. For details, see page 74.
`bgp` Displays BGP Information Menu. To view menu options, see page 76.
`ospf` Displays OSPF routing Information Menu. For details, see page 78.

Table 32. Layer 3 Information Options (/info/l3)

Command Syntax and Usage
`ospf3` Displays OSPFv3 routing Information Menu. For details, see page 82.
`rip` Displays Routing Information Protocol Menu. For details, see page 87.
`route6` Displays the IPv6 Routing information menu. To view menu options, see page 88.
`nbrcache` Displays the IPv6 Neighbor Discovery cache information menu. To view menu options, see page 89.
`ndprefix` Displays the IPv6 Neighbor Discovery Prefix information menu. To view menu options, see page 90.
`ecmp` Displays information about ECMP static routes. For details, see page 90.
`hash` *<Source IP address> <destination IP address> <number of ECMP paths>* Displays information about ECMP hashing results. For details, see page 90.
`ip` Displays IP Information. For details, see page 98. 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 91.
`mld` Displays MLD Information Menu. For details, see page 93.
`vrrp` Displays VRRP Information. For details, see page 96.
`if` Displays interface information. For details, see page 97.
`ip6pmtu` [*<destination IPv6 address>*] Displays IPv6 Path MTU information. For details, see page 97.

Table 32. Layer 3 Information Options (/info/l3)

Command Syntax and Usage
`ip` Displays IP Information. For details, see page 98. 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 99.
`ipsec` Displays IPsec Information menu. For details, see page 101.
`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
     best     - Show best routes
     ecmphash - Show the ECMP hash value
     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 33. 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 34 on page 72.
`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 35 on page 73.
`if` *<interface number>* Displays routes on a single interface.
`best` Displays the best routes. For more information, see page 72.
`ecmphash` Displays the current ECMP hashing mechanism.
`dump` Displays all routes configured in the switch. For more information, see page 72.

/info/l3/route/best

Show Best IP Route Information

```
Status code: * - best
    Destination         Mask          Gateway        Type      Tag      Metric   If
  --------------- --------------- --------------- --------- --------- ---------- --
* 0.0.0.0         0.0.0.0         172.25.1.1      indirect  static                1
* 10.90.90.0      255.255.255.0   10.90.90.81     direct    fixed               128
* 10.90.90.81     255.255.255.255 10.90.90.81     local     addr                128
* 10.90.90.255    255.255.255.255 10.90.90.255    broadcast broadcast           128
* 127.0.0.0       255.0.0.0       0.0.0.0         martian   martian
* 172.25.0.0      255.255.0.0     172.25.38.38    direct    fixed                 1
* 172.25.38.38    255.255.255.255 172.25.38.38    local     addr                  1
* 172.25.255.255  255.255.255.255 172.25.255.255  broadcast broadcast             1
* 224.0.0.0       224.0.0.0       0.0.0.0         martian   martian
* 224.0.0.0       240.0.0.0       0.0.0.0         multicast addr
* 255.255.255.255 255.255.255.255 255.255.255.255 broadcast broadcast
```

/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 34. 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 35. 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 GbESM.
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 36), VLAN and port for the address, and port referencing information.

Table 36. 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.
`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 75.

/info/l3/arp/dump

Show All ARP Entry Information

```
Total number of arp entries : 3
    IP address    Flags    MAC address    VLAN  Age Port
  --------------- ----- ----------------- ----  --- ----
  10.90.90.81      P    00:25:03:1f:fa:00 4095
  172.25.1.1            fc:cf:62:10:b2:00    1    1 EXT11
  172.25.38.38     P    00:25:03:1f:fa:00    1
```

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

The `Flag` field is interpreted as follows:

Table 37. 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
  --------------- --------------- -----------------  ---- -----
  172.25.38.38    255.255.255.255 00:25:03:1f:fa:00     1
  10.90.90.81     255.255.255.255 00:25:03:1f:fa:00  4095
```

/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 38. BGP Peer Information Menu Options (/info/l3/bgp)

Command Syntax and Usage
`peer` Displays BGP peer information. See page 76 for a sample output.
`summary` Displays peer summary information such as AS, message received, message sent, up/down, state. See page 77 for a sample output.
`peerrt` Displays BGP peer routes. See page 77 for a sample output.
`dump` Displays the BGP routing table. See page 77 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 ON
BGP router identifier 1.1.1.2, local AS number 100
BGP thid 24, allocs 1863, frees 917, current 218910, largest 4115
BGP Peer Summary Information:
BGP Static Peers:
        Peer         V    AS     MsgRcvd  MsgSent Up/Down   State
     --------------- - -------- -------- -------- -------- ------------------
  1: 10.10.10.4      4      200        6        6 00:06:01 established
  2: 11.11.11.2      4      300        3        2 00:01:01 established

BGP Dynamic Peers:
        Peer         V    AS     MsgRcvd  MsgSent Up/Down   Group
     --------------- - -------- -------- -------- -------- ------
 97: 192.168.128.4   4      200      290      290 04:44:25      1
 98: 192.168.129.4   4      200      290      290 04:44:24      2
```

/info/l3/bgp/peerrt

BGP Peer Routes Information

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

```
Current BGP neighbor 2 routes:
 Status codes: * valid, > best, = multipath, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete
    Network         Mask            Next Hop        Metr LcPrf  Wght  Path
   --------------- --------------- --------------- ----- ----- -----
------------------
*> 3.3.3.0         255.255.255.0   11.11.11.2                   128 300 i
*> 2.2.2.0         255.255.255.0   11.11.11.2                   128 300 i
*> 1.1.1.0         255.255.255.0   11.11.11.2                   128 300 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        Metr 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 39. OSPF Information Menu Options (/info/l3/ospf)

Command Syntax and Usage
`general` Displays general OSPF information. See page 79 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 79 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 80 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 80.
`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 39. OSPF Information Menu Options (/info/l3/ospf)

Command Syntax and Usage
routes Displays OSPF routing table. See page 82 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 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/loopif <*interface number*>

OSPF Interface Loopback Information

```
Ip Address 5.5.5.5, Area 0.0.0.1, Passive interface, Admin Status UP
Router ID 1.1.1.2, 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 40. 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.

Table 40. OSPF Database Information Menu Options (/info/l3/ospf/dbase)

Command Syntax and Usage
`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`.
`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 41. 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 84.
`dbase` Displays the OSPFv3 database menu. To view menu options, see page 86.
`areas` Displays the OSPFv3 Area Table.

Table 41. 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 85.
`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 87.
`borderrt` Displays OSPFv3 routes to an ABR or ASBR.
`dump` Displays all OSPFv3 information. To view a sample display, see page 85.

/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 42. 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 43. 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 44. RIP Information Menu Options (/info/l3/rip)

Command Syntax and Usage
routes Displays RIP routes. For more information, see page 87.
dump *<interface number or zero for all IFs)>* Displays RIP user's configuration. For more information, see page 88.

/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 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 45 describes the IPv6 Routing information options.

Table 45. 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 34 on page 72.
`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 89.

/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 46 describes IPv6 Neighbor Discovery cache information menu options.

Table 46. 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 90.

/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
```

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: 10.10.10.10
Enter DIP address (0 for SIP only): 157.0.0.10
Enter number of ECMP paths: 32
Source 10.10.10.10 will go through route number 9
```

ECMP hashing information shows the status of ECMP hashing on each switch.

/info/l3/igmp

IGMP Multicast Group Information Menu

```
[IGMP Multicast Menu]
     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 47 describes the commands used to display information about IGMP groups learned by the switch.

Table 47. IGMP Multicast Group Information Menu Options (/info/l3/igmp)

Command Syntax and Usage
`mrouter` Displays IGMP Multicast Router menu. To view menu options, see page 92.
`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 92
`ipmcgrp` *<VLAN number>* Displays all ipmc groups on a single VLAN.

/info/l3/igmp/mrouter
IGMP Multicast Router Port Information Menu

```
[IGMP Multicast Router Menu]
     vlan     - Show all multicast router ports on a single vlan
     dump     - Show all learned multicast router ports
```

Table 48 describes the commands used to display information about multicast routers (Mrouters) learned through IGMP Snooping.

Table 48. 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.
`dump` Displays information for all multicast groups learned by the switch.

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

```
Total entries: 1 Total number of dynamic mrouters: 1
SrcIP               VLAN    Port       Version   Expires   MRT       QRV   QQIC
------------------- ------- -------    --------- --------  -------   ----  ----
172.25.110.199      1       EXT11      V2        3:06      10        0     0
```

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

```
Total entries: 1007  Total IGMP groups: 1007
Note: The <Total IGMP groups> number is computed as
      the number of unique (Group, Vlan) entries!
Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.
     Source         Group       VLAN    Port   Version   Mode  Expires  Fwd
 -------------- --------------- ------- ------ --------  ----- -------  ---
 10.1.1.1       232.1.1.1         2      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/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 49 describes the MLD information menu options.

Table 49. MLD Information Menu Options (/info/l3/mld)

Command Syntax and Usage
`mrouter` Displays MLD Mrouter information menu. To view menu options, see page 94.
`groups` Displays all MLD groups.
`find` *<IP6 address>* Displays a single MLD group by its IP address.

Table 49. MLD Information Menu Options (/info/l3/mld)

Command Syntax and Usage
`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 50 describes the commands used to display information about MLD Mrouter ports.

Table 50. MLD Mrouter Information Menu Options (/info/l3/mld/mrouter)

Command Syntax and Usage
`dump` Displays information for MLD Mrouter ports. See page 95 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 51 describes the MLD Mrouter dump information displayed in the output.

Table 51. 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 GbESM 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:
  1: IP4 127.31.35.5     255.255.0.0  127.31.255.255,  vlan 1, up
  2: IP6 2002:0:0:0:0:0:0:5/64                       , vlan 1, up
         fe80::213:aff:fe4f:7c01
  3: IP6 3003:0:0:0:0:0:0:5/64                       , vlan 2, up
         fe80::213:aff:fe4f:7c02
127: IP6 10:90:90:0:0:0:0:97/64                      , vlan 4095, DOWN
128: IP4 10.90.90.97    255.255.255.0   10.90.90.255,  vlan 4095, up
```

For each interface, the following information is displayed:

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

/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:
127: IP6 0:0:0:0:0:0:0:0/0                              , vlan 4095, up
         fe80::218:b1ff:fe31:8400
128: IP4 172.25.160.3    255.255.0.0     172.25.255.255,  vlan 4095, up

Loopback interface information:

Default gateway information: metric strict
132: 172.25.1.1,      up  active

Default IP6 gateway information:

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

Current BOOTP relay option-82 settings: OFF
Current BOOTP relay option-82 policy: Replace

Current DHCP Snooping settings: Off
DHCP Snooping is configured on the following VLANs:
 empty
Insertion of option 82 information is Disable
      Interface   Trusted    Rate limit (pps)
-----------------------------------
           INT1        No                none
           INT2        No                none
...
           EXT8        No                none
           EXT9        No                none

Current IP forwarding settings: ON, dirbr disabled, noicmprd disabled, ICMPv6
redirect disabled

RIP is disabled.

OSPF is disabled.

OSPFv3 is disabled.

BGP 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 52 describes the commands used to display information about IKEv2.

Table 52. IKEv2 Information Menu Options (/info/l3/ikev2)

Command Syntax and Usage
`info` Displays all IKEv2 information. See page 100 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 53 describes the commands used to display information about IPsec.

Table 53. 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 102 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
     advbuf   - Show Advanced Buffer Management configuration
```

Table 54. QoS Menu Options (/info/qos)

Command Syntax and Usage
`8021p` Displays 802.1p information. For details, see page 103.
`advbuf` Displays Advanced Buffer Management configuration information. For details, see page 104.

/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
-----  --------  ----  ------
INT1        0       0      1
INT2        0       0      1
...
MGT1        0       0      1
MGT2        0       0      1
EXT1        0       0      1
EXT2        0       0      1
EXT3        0       0      1
EXT4        0       0      1
...
```

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

Table 55. 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 56. 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/advbuf

Advanced Buffer Management Information

```
Ingress buffer policy configuration:
* 0 means default. Number of cell/discard shown in KBytes

 Port     Packet:reset        Cell:reset        Discard
-----     ------------       -----------        -------
INT1      0     :0           0    :0            0
INT2      0     :0           0    :0            0
..
EXT8      0     :0           0    :0            0
EXT9      0     :0           0    :0            0

Egress buffer policy configuration:
* 0 means default. Number of cell/shared cell shown in KBytes

        Total shared cell per chip: 0. Reset Value: 0

 Port     Packet:reset:Q      Cell:reset:Q      Shared:reset
-----     --------------     -------------      ------------
INT1      0     :0    :1     0    :0    :1      0     :0
          0     :0    :2     0    :0    :2
INT2      0     :0    :1     0    :0    :1      0     :0
          0     :0    :2     0    :0    :2
...
EXT8      0     :0    :1     0    :0    :1      0     :0
          0     :0    :2     0    :0    :2
EXT9      0     :0    :1     0    :0    :1      0     :0
          0     :0    :2     0    :0    :2
```

/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 57. ACL Information Menu Options (/info/acl)

Command Syntax and Usage
`acl-list` *<ACL number>* Displays ACL list information. For details, see page 106.
`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
   Meter
     - Set to disabled
     - Set committed rate : 64
     - Set max burst size : 32
   Re-Mark
     - Set use of TOS precedence to disabled
   Actions        : Permit
   Statistics     : enabled
```

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

Table 58. ACL List Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Meter	Displays the ACL meter parameters.
Re-Mark	Displays the ACL re-mark parameters.
Actions	Displays the configured action for the ACL.
Statistics	Displays the status of ACL statistics configuration (enabled or disabled).

/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 59. RMON Information Menu Options (/info/rmon)

Command Syntax and Usage
`hist` Displays RMON History information. For details, see page 108.
`alarm` Displays RMON Alarm information. For details, see page 109.
`event` Displays RMON Event information. For details, see page 110.
`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 60. 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 61. 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.
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 62. 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
----   -----   -----   --------  --TX-----RX--   ------
 INT1    1      1000     full     yes    yes       up
 INT2    2      1000     full     yes    yes       up
 INT3    3      1000     full     yes    yes       up
 INT4    4      1000     full     yes    yes       up
 INT5    5      1000     full     yes    yes      down
 INT6    6      1000     full     yes    yes       up
 INT7    7      1000     full     yes    yes       up
 INT8    8      1000     full     yes    yes       up
 INT9    9      1000     full     yes    yes       up
 INT10  10      1000     full     yes    yes       up
 INT11  11      1000     full     yes    yes       up
 INT12  12      1000     full     yes    yes       up
 INT13  13      1000     full     yes    yes       up
 INT14  14      1000     full     yes    yes       up
 MGT1   15       100     full     yes    yes       up
 MGT2   16       100     full     yes    yes       up
 EXT1   17     10000     full     yes    yes      down
 EXT2   18     10000     full     yes    yes      down
 EXT3   19     10000     full     yes    yes     disabled
 EXT4   20       any      any     yes    yes      down
 EXT5   21       any      any     yes    yes      down
 EXT6   22       any      any     yes    yes      down
 EXT7   23       any      any     yes    yes      down
 EXT8   24       any      any     yes    yes      down
 EXT9   25       any      any     yes    yes      down
```

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

Use this command to display link status information about each port on a GbESM 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    Type    Fast RMON Lrn Fld PVID     NAME            VLAN(s)
----- ---- --- --------- ---- ---- --- --- ----- -------------- ----------------
INT1  1     y  Internal   n    d    e   e     1  INT1           1
INT2  2     y  Internal   n    d    e   e     1  INT2           1
INT3  3     y  Internal   n    d    e   e     1  INT3           1
INT4  4     y  Internal   n    d    e   e     1  INT4           1
INT5  5     y  Internal   n    d    e   e     1  INT5           1
INT6  6     y  Internal   n    d    e   e     1  INT6           1
INT7  7     y  Internal   n    d    e   e     1  INT7           1
INT8  8     y  Internal   n    d    e   e     1  INT8           1
INT9  9     y  Internal   n    d    e   e     1  INT9           1
INT10 10    y  Internal   n    d    e   e     1  INT10          1
INT11 11    y  Internal   n    d    e   e     1  INT11          1
INT12 12    y  Internal   n    d    e   e     1  INT12          1
INT13 13    y  Internal   n    d    e   e     1  INT13          1
INT14 14    y  Internal   n    d    e   e     1  INT14          1
MGT1  15    y  Mgmt       n    d    e   e  4095* MGT1           4095
MGT2  16    y  Mgmt       n    d    e   e  4095* MGT2           4095
EXT1  17    n  External   n    d    e   e     1  EXT1           1
EXT2  18    n  External   n    d    e   e     1  EXT2           1
EXT3  19    n  External   n    d    e   e     1  EXT3           1
EXT4  20    n  External   n    d    e   e     1  EXT4           1
...
* = 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 BladeCenter unit that you are using and the firmware versions and options that are installed.

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Type of port (Internal, External, or Management)
- Whether the port is configured for Port Fast Fowarding (`Fast`)
- 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

```
------------------------------------------------------------------------
   Port     Device  TXEna RXSig TXuW  RXuW  TXFlt Vendor           Serial
---------- ------- ----- ----- ----- ----- ----- ---------------- --------
 17 -  EXT1 CU SFP  Ena   Down   N/A   N/A  none  Blade Network    BNT083ZFS
 18 -  EXT2 3m DAC  Ena   Down   N/A   N/A  none  Molex Inc.       822630025
 19 -  EXT3 SR SFP+ Ena   Down  555.1   0.9 none  Blade Network    AD072E0L3
```

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

- Port number and media type
- TXEna: Transmission status
- RXsig: Receive Signal indicator
- TXuW: Transmit power, in micro-watts
- RXuW: Receive power, in micro-watts
- TXflt: Transmission fault indicator
- Vendor name
- Serial number

The optical power levels shown for transmit and receive functions for the transceiver must 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 63. 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 μW in this table to match the unit of measure shown in the `/info/transcvr` output.

/info/virt

Virtualization Information

```
[Virtualization Menu]
     vm       - Show Virtual Machine information
```

Table 64 describes general virtualization information options. More details are available in the following sections.

Table 64. Virtualization Information Options (/info/virt)

Command Syntax and Usage
vm Displays the Virtual Machines (VM) information menu. For details, see page 114.

/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 65. 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 *<trunk group number>* Displays Virtual Machine information for the selected trunk.
dump Displays all Virtual Machine information. For details, see page 115.

/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 66. VMware Information Options (/info/virt/vm/vmware)

Command Syntax and Usage
`hosts` Displays a list of VMware hosts. For details, see page 116.
`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/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 5. 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
     snmp     - Show SNMP stats
     ntp      - Show NTP stats
     clrmp    - Clear all MP related stats
     clrports - Clear stats for all ports
     dump     - Dump all stats
```

The information provided by each menu option is briefly described in Table 67, with pointers to detailed information.

Table 67. 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 119.
`trunk` *<trunk group number>* Displays the Trunk Statistics Menu for the specified port. To view menu options, see page 142.
`l2` Displays the Layer 2 Statistics Menu. To view menu options, see page 142.
`l3` Displays the Layer 3 Stats Menu. To view menu options, see page 149.
`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 183.
`acl` Displays ACL Statistics menu. To view menu options, see page 195.

Table 67. Statistics Menu Options (/stats)

Command Syntax and Usage
`snmp` Displays SNMP statistics. See page 197 for sample output.
`ntp [clear]` Displays Network Time Protocol (NTP) Statistics. See page 201 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.
`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 201.

/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
     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 68. Port Statistics Menu Options (/stats/port)

Command Syntax and Usage
`8021x` Displays IEEE 802.1x authenticator statistics for the port. See page 122 for sample output.
`bootp` Displays BOOTP Relay statistics for the port. See page 124 for sample output.
`brate` Displays continuous interface bitrate usage in Kb per second.
`brg` Displays bridging (“dot1”) statistics for the port. See page 125 for sample output.
`brg-rate` Displays bridging (“dot1”) statistics per second for the port. See page 126 for sample output.
`ether` Displays Ethernet (“dot3”) statistics for the port. See page 126 for sample output.
`eth-rate` Displays Ethernet (“dot3”) statistics per second for the port. See page 126 for sample output.

Table 68. Port Statistics Menu Options (/stats/port) (continued)

Command Syntax and Usage
`if` Displays interface statistics for the port. See page 133 for sample output.
`if-rate` Displays interface statistics per second for the port. See page 136 for sample output.
`ip` Displays IP statistics for the port. See page 137 for sample output.
`ip-rate` Displays IP statistics per second for the port. See page 139 for sample output.
`link` Displays link statistics for the port. See page 139 for sample output.
`maint` Displays detailed maintenance statistics for the port.
`rmon` Displays Remote Monitoring (RMON) statistics for the port. See page 140 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 69. 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 70. 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 70. 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x) (continued)

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 70. 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x) (continued)

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 bootstrap protocol relay statistics of the selected port

```
BOOTP Relay statistics for port EXT11:

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 INT1:
dot1PortInFrames:                   63242584
dot1PortOutFrames:                  63277826
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 71. 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*>/brg-rate

Bridging Per Second Statistics

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

```
Bridging statistics for port INT1A:
dot1PortInFrames:                          0
dot1PortOutFrames:                         0
dot1PortInDiscards:                        0
dot1TpLearnedEntryDiscards:                0
dot1StpPortForwardTransitions:             0
```

Table 72. 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 ethernet statistics of the selected port.

```
Ethernet statistics for port INT1A:
dot3StatsAlignmentErrors:                  0
dot3StatsFCSErrors:                        0
dot3StatsSingleCollisionFrames:            0
dot3StatsMultipleCollisionFrames:          0
dot3StatsLateCollisions:                   0
dot3StatsExcessiveCollisions:              0
dot3StatsInternalMacTransmitErrors:       NA
dot3StatsFrameTooLongs:                    0
dot3StatsInternalMacReceiveErrors:         0
```

Table 73. Ethernet Statistics of a Port (/stats/port/ether)

Statistics	Description
dot3StatsAlignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsFCS Errors	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.
dot3StatsSingle CollisionFrames	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.

Table 73. Ethernet Statistics of a Port (/stats/port/ether)

Statistics	Description
dot3StatsMultiple CollisionFrames	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.
dot3StatsLate Collisions	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.
dot3StatsExcessiv e Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternal MacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3StatsCarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 73. Ethernet Statistics of a Port (/stats/port/ether)

Statistics	Description
dot3StatsFrameTo o 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.
dot3StatsInternal MacReceiveErrors	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*>/eth-rate

Ethernet Statistics Per Second

This menu option enables you to display the ethernet statistics per second of the selected port.

```
Ethernet statistics for port INT1A:
dot3StatsAlignmentErrors:                  0
dot3StatsFCSErrors:                        0
dot3StatsSingleCollisionFrames:            0
dot3StatsMultipleCollisionFrames:          0
dot3StatsLateCollisions:                   0
dot3StatsExcessiveCollisions:              0
dot3StatsInternalMacTransmitErrors:       NA
dot3StatsFrameTooLongs:                    0
dot3StatsInternalMacReceiveErrors:         0
```

Table 74. Ethernet Statistics of a Port (/stats/port/ether)

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.

Table 74. Ethernet Statistics of a Port (/stats/port/ether) (continued)

Statistics	Description
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollisionFrame` object.
dot3StatsMultipleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollisionFrames` object.
dot3StatsLateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMac TransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3StatsCarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.

Table 74. Ethernet Statistics of a Port (/stats/port/ether) (continued)

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

/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

Empty Egress Portmap:          3085 *
* Check for "HOL-blocking" discards on associated egress ports
```

Table 75. 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 75. 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).

Table 75. Interface Statistics of a Port (/stats/port/if)

Statistics	Description
Policy Discards	Dropped due to policy setting, such as a user-configured static entry.
Non-Forwarding State	Discarded because the ingress port is not in the forwarding state.
IBP/CBP Discards	Discarded because of Ingress Back Pressure (flow control), or because the Common Buffer Pool is full (for example, insufficient packet buffering).
HOL-blocking Discards	Discarded because of the Head Of Line (HOL) blocking mechanism. Low-priority packets are placed in a separate queue and can be discarded while applications or the TCP protocol determine whether a retransmission is necessary. HOL blocking forces transmission to stop until the overloaded egress port buffer can receive data again.
MMU Discards	Discarded because of the Memory Management Unit.
Cell Error Discards	
MMU Aging Discards	
Other Discards	Discarded packets not included in any category.

/stats/port <*port alias or number*>/if-rate
Interface Statistics Per Second

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

```
Interface statistics for port INT1A:
                     ifHCIn Counters       ifHCOut Counters
Octets:                            0                      0
UcastPkts:                         0                      0
BroadcastPkts:                     0                      0
MulticastPkts:                     0                      0
FlowCtrlPkts:                      0                      0
Discards:                          0                      0
Errors:                            0                      0
```

Table 76. Interface Statistics of a Port (/stats/port/if-rate)

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.
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.

Table 76. Interface Statistics of a Port (/stats/port/if-rate) (continued)

Statistics	Description
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.

/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 INT1:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 77. 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*>/ip-rate
Interface Protocol Per Second Statistics

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

```
GEA IP statistics for port INT1A:
ipInReceives   :         0
ipInHeaderError:         0
ipInDiscards   :         0
```

Table 78. 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 INT1:
linkStateChange:            1
```

Table 79. 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 80. 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.
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.

Table 80. RMON Statistics of a Port (/stats/port/rmon)

Statistics	Description
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
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 81. 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]
     amp      - AMP Stats Menu
     fdb      - Show FDB stats
     lacp     - Show LACP stats
     hotlink  - Show Hot Links stats
     lldp     - Show LLDP port stats
     oam      - Show OAM stats
```

The Layer 2 statistics provided by each menu option are briefly described in Table 82, with pointers to detailed information.

Table 82. Layer 2 Statistics Menu Options (/stats/l2)

Command Syntax and Usage
`amp` Displays Active MultiPath (AMP) statistics. See page 143 for sample output.
`fdb [clear]` Displays FDB statistics. See page 144 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 145 for sample output. Use the `clear` option to delete all LACP statistics.
`hotlink` Displays Hotlinks statistics. See page 146 for sample output.

Table 82. Layer 2 Statistics Menu Options (/stats/l2)

Command Syntax and Usage
`lldp` [<*port alias or number*>|`clear`] Displays LLDP port statistics for a specified port or for all ports if no port is specified. See page 147 for sample output. Use the `clear` option to delete all LLDP statistics.
`oam` Displays the OAM Statistics menu. See page 147 for sample output.

/stats/l2/amp
Active MultiPath Statistics

```
[AMP Statistics Menu]
     group    - Show AMP group stats
     dump     - Show all AMP port stats
     clear    - Clear AMP stats
```

The following table describes the AMP statistics commands:

Table 83. AMP Statistics Options

Command Syntax and Usage
`group` [<*AMP group number*>] Displays AMP statistics for the selected group. See page 144 for sample output.
`dump` Displays all AMP statistics.
`clear` [<*AMP group number*>] Clears AMP statistics.

/stats/l2/amp/group [<*AMP group number*>]

Active MultiPath Group Statistics

```
                    Keep-alive Pkts       Fdb-Flush  Pkts         Pkts
Group      Link     Sent       Rcvd       Sent       Rcvd        Dropped
-----  -----------  ---------- ---------- ---------- ---------- ---------
1      Port EXT1    26         0          0          0          0
       Port EXT2    0          0          0          0          0
```

This displays shows AMP group statistics for an access switch. AMP statistics are described in the following table:

Table 84. AMP Statistics

Statistic	Description
Group	AMP group number.
Link	Ports/portchannels (trunks) used for the AMP link.
Keep-alive Pkts Sent	Number of keep-alive packets sent.
Keep-alive Pkts Rcvd	Number of keep-alive packets received.
Fdb-Flush Pkts Sent	Number of FDB-flush packets sent.
Fdb-Flush Pkts Rcvd	Number of FDB-flush packets received.
Packets Dropped	Number of invalid AMP packets dropped.

/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 85. 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

```
LACP statistics for port INT1:
 -------------------------------------
 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 86. 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.
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 87. 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 INT1 Statistics
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Frames Transmitted          : 0
Frames Received             : 0
Frames Received in Errors   : 0
Frames Discarded            : 0
TLVs Unrecognized           : 0
Neighbors Aged Out          : 0
```

The following table describes the LLDP port statistics:

Table 88. 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 89. 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 148 for sample output.
dump Displays all OAM statistics.

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

OAM Statistics

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

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

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

OAM statistics include the following:

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

/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
     dhcp     - DHCP statistic Menu
     dump     - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in Table 90, with pointers to detailed information.

Table 90. 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. See page 152 for sample output.
`ip` Displays IP statistics. See page 153 for sample output.
`ip6` Displays IPv6 statistics. See page 156 for sample output.
`route [clear]` Displays IPv4 route statistics. See page 160 for sample output. Use the `clear` option to delete all route statistics.

Table 90. Layer 3 Statistics Menu Options (/stats/l3) (continued)

Command Syntax and Usage
`route6 [clear]` Displays IPv6 route statistics. See page 161 for sample output. Use the `clear` option to delete all route statistics.
`pmtu6` Displays IPv6 Path MTU statistics. See page 161 for sample output.
`arp` Displays Address Resolution Protocol (ARP) statistics. See page 162 for sample output.
`dns [clear]` Displays Domain Name System (DNS) statistics. See page 162 for sample output. Use the `clear` option to delete all DNS statistics.
`icmp [clear]` Displays ICMP statistics. See page 163 for sample output. Use the `clear` option to delete all ICMP statistics.
`tcp [clear]` Displays TCP statistics. See page 165 for sample output. Use the `clear` option to delete all TCP statistics.
`udp [clear]` Displays UDP statistics. See page 166 for sample output. Use the `clear` option to delete all UDP statistics.
`igmp` Displays IGMP statistics. See page 167 for sample output.
`mld` Displays the MLD statistics menu. See page 168 for menu options.
`ospf` Displays OSPF statistics. See page 171 for sample output.
`ospf3` Displays OSPFv3 statistics. See page 176 for sample output.
`vrrp` When virtual routers are configured, you can display the protocol statistics for VRRP. See page 181 for sample output.
`rip` Displays Routing Information Protocol (RIP) statistics. See page 182 for sample output.

Table 90. Layer 3 Statistics Menu Options (/stats/l3) (continued)

Command Syntax and Usage
`igmpgrps` Displays the total number of IGMP groups that are registered on the switch.
`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.
`dhcp` 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.
`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/geal3

Gigabit Ethernet Aggregators (GEA) Statistics

```
[GEA Layer 3 Statistics Menu]
     l3bucket - Show GEA L3 bucket for an IP address
     dump     - Dump GEA layer 3 stats counter
```

The following table describes the GEA statistics. These are used by technical and support personnel.

Table 91. Layer 3 GEA Statistics Menu Options (/stats/l3/geal3)

Command Syntax and Usage
`l3bucket` *<IP address>* Displays the GEA L3 bucket for the specified IP address.
`dump` Displays the GEA layer 3 statistics counter.

/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 92. 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.

Table 92. IPv4 Statistics (stats/l3/ip) (continued)

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

Table 92. IPv4 Statistics (stats/l3/ip) (continued)

Statistics	Description
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

/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 93. 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.
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.

Table 93. IPv6 Statistics (stats/l3/ip6) (continued)

Statistics	Description
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.
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).

Table 93. IPv6 Statistics (stats/l3/ip6) (continued)

Statistics	Description
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 94. 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.
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.

Table 94. ICMP Statistics (stats/l3/ip6) (continued)

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

The following table describes the UDP statistics.

Table 95. 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     :            3
Highest number ever recorded         :            3
Current static routes                :            1
Current RIP routes                   :            0
Current OSPF routes                  :            0
Current BGP routes                   :            0
Maximum supported routes             :         2048

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

Table 96. IPv4 Route Statistics (/stats/l3/route)

Statistics	Description
Current total outstanding routes	The total number of outstanding routes in the route table.
Highest number ever recorded	The highest number of routes ever recorded in the route table.
Current static routes	The number of static routes in the route table.
Current RIP routes	The number of RIP routes in the route table.
Current OSPF routes	The number of OSPF routes in the route table.
Current BGP routes	The number of BGP routes in the route table.
Maximum supported routes	The maximum number of routes that are supported.
Maximum number of ECMP routes	The maximum number of ECMP routes supported.
Maximum number of static ECMP routes	The maximum number of static ECMP routes supported.
Number of routes with ECMP paths	The number of routes with ECMP paths.

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 97. 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 98. 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 99. 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 100. DNS Statistics (/stats/l3/dns)

Statistics	Description
dnsInRequests	The total number of DNS request 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 101. 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.

Table 101. ICMP Statistics (/stats/l3/icmp) (continued)

Statistics	Description
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
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 102. 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 102. 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 103. 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 1 statistics:
------------------------------------------------------------------
rxIgmpValidPkts:                  51222   rxIgmpInvalidPkts:                0
rxIgmpGenQueries:                  1378   rxIgmpGrpSpecificQueries:      3896
rxIgmpGroupSrcSpecificQueries:        0   rxIgmpDiscardPkts:                0
rxIgmpLeaves:                      1949   rxIgmpReports:                43999
txIgmpReports:                        0   txIgmpGrpSpecificQueries:         2
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 104. 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 105 describes the MLD statistics menu options.

Table 105. MLD Statistics Menu (/stats/l3/mld)

Command Syntax and Usage
`global` Displays MLD global statistics. See page 169 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 106. 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 107. OSPF Statistics Menu (/stats/l3/ospf)

Command Syntax and Usage
`general` Displays global statistics. See page 172 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 108. 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 108. 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 108. 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 108. 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 109. OSPFv3 Statistics Menu (/stats/l3/ospf3)

Command Syntax and Usage
`general` Displays global statistics. See page 177 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 110. 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 110. 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 110. 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.
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.

Table 110. OSPFv3 General Statistics (stats/l3/ospf3/general) (continued)

Statistics	Description
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 1/10Gb Uplink ESM (GbESM) 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 111. 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 112. 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 184.
`tcb` Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 192.
`ucb` Displays all UDP control blocks that are in use. To view a sample output, see page 193.
`cpu` Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the statistics, see page 193.
`ncpu` 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 194.

Table 112. Management Processor Statistics Menu Options (/stats/mp)

Command Syntax and Usage
`hcpu` Displays CPU utilization history. To view a sample output and a description of the stats, see page 195.
`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 113. Management Processor Statistics Menu Options (/stats/mp)

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 193.
`clear` Clears all CPU packet statistics and logs.
`logs` Displays log of all packets received by CPU.
`last` Displays log of last the N packets received by CPU.
`dump` Dumps all packet statistics and logs.
`parse` Displays the MP Packet Parse menu. To view options, see page 188.

/stats/mp/pkt/counters

MP Packet Statistics

```
 CPU packet statistics at 18:57:14 Thu Nov 10, 2011

 Packets received by CPU:
 ------------------------
 Total packets:          58922 (58922 since bootup)
 BPDUs:                   4910
 Cisco packets:              0
 ARP packets:            45777
 IPv4 packets:            8066
 IPv6 packets:            4301
 LLDP PDUs:                165
 Other:             4294962999

Packet Buffer Statistics:
-------------------------
 allocs:         74315
 frees:          74314
 failures:           0
 dropped:            0

 small packet buffers:
 ---------------------
   current:                  0
   max:                   1024
   threshold:              128
   hi-watermark:             2
   hi-water time:   17:35:17 Thu Nov 10, 2011

 medium packet buffers:
 ----------------------
   current:                  1
   max:                    400
   threshold:               50
   hi-watermark:            20
   hi-water time:   17:39:03 Thu Nov 10, 2011

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

 pkt_hdr statistics:
 ---------------------
 current          :           0
 max              :        3072
 hi-watermark     :          23
```

Table 114. MP Packet Statistics (/stats/mp/pkt/counters)

Statistics	Description
Packets received by CPU	
Total packets	Total number of packets received
BPDUs	Total number of spanning-tree Bridge Protocol Data Units received.
Cisco packets	Total number of UniDirectional Link Detection (UDLD) packets and Cisco Discovery Protocol (CDP) packets received.
ARP packets	Total number of Address Resolution Protocol packets received.
IPv4 packets	Total number of IPv4 packets received.
IPv6 packets	Total number of IPv6 packets received.
LLDP PDUs	Total number of Link Layer Discovery Protocol data units received.
Other	Total number of other packets received.
Packet Buffer Statistics	
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
small packet buffers	
current	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of small packet allocations supported
threshold	Threshold value for small packet allocations, beyond which only high-priority small packets are allowed.
hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.

Table 114. MP Packet Statistics (/stats/mp/pkt/counters) (continued)

Statistics	Description
medium packet buffers	
current	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Threshold value for medium packet allocations, beyond which only high-priority medium packets are allowed.
threshold	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-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
hi-water time	Time stamp that indicates when the hi-watermark was reached.
jumbo packet buffers	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of jumbo packet allocations supported.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
pkt_hdr statistics	
current	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
max	Maximum number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IPprotocol stack.
hi-watermark	The highest number of packet allocation with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

/stats/mp/pkt/parse

MP Packet Parse Menu

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

Table 115. Packet Statistics Menu Options

Command Syntax and Usage
`rx` Displays the Packet-log Parse Types menu. For a list of options ,see page 189.
`tx` Displays the Packet-log Parse Types menu. For a list of options ,see page 189.

/stats/mp/pkt/parse/rx
/stats/mp/pkt/parse/tx

MP Packet-log Parse Types Menu

```
[MP Packet-log Parse Types Menu]
     arp      - Display only ARP packets logged
     rarp     - Display only Reverse-ARP packets
     bpdu     - Display only BPDUs logged
     cisco    - Display only Cisco packets (BPDU/CDP/UDLD) logged
     lacp     - Display only LACP PDUs logged
     fcoe     - Display only FCoE FIP PDUs logged
     ipv4     - Display only IPv4 packets logged
     igmp     - Display only IGMP packets logged
     pim      - Display only PIM packets logged
     icmp     - Display only ICMP packets logged
     tcp      - Display only TCP packets logged
     ftp      - Display only FTP packets logged
     http     - Display only HTTP packets logged
     ssh      - Display only SSH packets logged
     tacacs   - Display only TACACS packets logged
     telnet   - Display only TELNET packets logged
     tcpother - Display only TCP other-port packets logged
     udp      - Display only UDP packets logged
     dhcp     - Display only DHCP packets logged
     ntp      - Display only NTP packets logged
     radius   - Display only RADIUS packets logged
     snmp     - Display only SNMP packets logged
     tftp     - Display only TFTP packets logged
     udpother - Display only UDP other-port packets logged
     ipv6     - Display only IPv6 packets logged
     rip      - Display only RIP packets logged
     ospf     - Display only OSPF packets logged
     bgp      - Display only BGP packets logged
     lldp     - Display only LLDP PDUs logged
     vlan     - Display only logged packets with specified vlan
     port     - Display only logged packets with specified port
     mac      - Display only logged packets with specified mac address
     ip-addr  - Display only logged packets with specified ip address
     other    - Display logs of all packets not explicitly selectable
     raw      - Display raw packet buffer in addition to headers
```

The behavior of the options in this menu is dependent upon the menu from which you arrived at the MP Packet-log Parse Types menu.

- If you arrived at this menu from `/stats/mp/pkt/parse/rx`, only received packets that have been parsed that fit the selected option are displayed.
- If you arrived at this menu from `/stats/mp/pkt/parse/tx`, only sent packets that have been parsed that fit the selected option are displayed.

Table 116 describes the parsing options.

Table 116. Packet Log Parsing Options

Command Syntax and Usage
`arp` Displays only ARP packets logged
`rarp` Displays only Reverse-ARP packets
`bpdu` Displays only BPDUs logged
`cisco` Displays only Cisco packets (BPDU/CDP/UDLD) logged
`lacp` Displays only LACP PDUs logged
`fcoe` Displays only FCoE FIP PDUs logged
`ipv4` Displays only IPv4 packets logged
`igmp` Displays only IGMP packets logged
`pim` Displays only PIM packets logged
`icmp` Displays only ICMP packets logged
`tcp` Displays only TCP packets logged
`ftp` Displays only FTP packets logged
`http` Displays only HTTP packets logged
`ssh` Displays only SSH packets logged
`tacacs` Displays only TACACS packets logged
`telnet` Displays only TELNET packets logged

Table 116. Packet Log Parsing Options (continued)

Command Syntax and Usage
`tcpother` Displays only TCP other-port packets logged.
`udp` Displays only UDP packets logged.
`dhcp` Displays only DHCP packets logged.
`ntp` Displays only NTP packets logged.
`radius` Displays only RADIUS packets logged.
`snmp` Displays only SNMP packets logged.
`tftp` Displays only TFTP packets logged.
`udpother` Displays only UDP other-port packets logged.
`ipv6` Displays only IPv6 packets logged.
`rip` Displays only RIP packets logged.
`ospf` Displays only OSPF packets logged.
`bgp` Displays only BGP packets logged.
`lldp` Displays only LLDP PDUs logged.
`vlan` <*VLAN_number*> Displays only logged packets with the specified VLAN.
`port` <*port_number*> Displays only logged packets with the specified port.
`mac` <*MAC_address*> Displays only logged packets with the specified MAC address.
`ip-addr` <*IPv4_address*> Displays only logged packets with the specified IPv4 address.

Table 116. Packet Log Parsing Options (continued)

Command Syntax and Usage
`other` Displays logs of all packets not explicitly selectable.
`raw` Displays raw packet buffer in addition to headers.

/stats/mp/tcb
TCP Statistics

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

Table 117. MP Specified TCP Statistics (/stats/mp/tcb)

Statistics	Description
14835bd8	Memory
0.0.0.0	Destination IP address
0	Destination port
172.31.38.107	Source IP
80	Source port
listen/MGT up	State

/stats/mp/ucb
UCB Statistics

```
Data Ports:
------------------------------------------------------------------
All UDP allocated control blocks:
   68:  listen
  161:  listen
  500:  listen
  546:  listen
```

/stats/mp/cpu
CPU Statistics

This menu option enables you to display the CPU use statistics.

```
       CPU utilization           Highest     Thread               Time
------------------------------   -------   ----------    -------------------------
cpuUtil1Second:            13%      93%    110 (FTMR)    11:36:19 Mon Oct 10, 2011
cpuUtil4Seconds:            7%
cpuUtil64Seconds:          13%
```

Table 118. CPU Statistics (stats/mp/cpu)

Statistics	Description
cpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
cpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
cpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.
Highest	The highest percent of CPU use.
Thread	The thread ID and name of the thread that caused the highest CPU use.
Time	The time when the highest CPU use was reached.

/stats/mp/ncpu

New CPU Statistics

This option displays CPU use statistics for all threads.

```
------------------------------------------------------------------------
Total CPU Utilization: For 1 second: 0.66%
                       For 5 second: 3.02%
                       For 1 minute: 3.73%
                       For 5 minute: 3.69%
Highest thread util  : 100% by  58 (I2C ) at 11:31:32 Sat Mar 10, 2012
------------------------------------------------------------------------
Thread  Thread                    Utilization                  Status
  ID     Name        1sec       5sec       1Min       5Min
------------------------------------------------------------------------
  1      STEM       0.00%      0.00%      0.00%      0.00%       idle
  2      STP        0.00%      0.00%      0.00%      0.00%       idle
  3      MFDB       0.00%      0.00%      0.00%      0.00%       idle
  4      TND        0.00%      0.00%      0.00%      0.00%       idle
  5      CONS       0.00%      0.01%      0.38%      0.08%    running
  6      TNET       0.00%      0.00%      0.00%      0.00%       idle
...
123      PBR        0.00%      0.00%      0.00%      0.00%       idle
124      HIST       0.00%      0.00%      0.00%      0.00%       idle
126      NORM       0.00%      0.00%      0.00%      0.00%       idle
127      DONE       0.00%      0.00%      0.00%      0.00%       idle
------------------------------------------------------------------------
```

Table 119. CPU Statistics

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

/stats/mp/hcpu
CPU Statistics History

This option displays a history of CPU use statistics.

```
-----------------------------------------
CPU Utilization History
-----------------------------------------
 17 (IP  )  98% at  22:17:24 Mon Feb 20, 2012
 59 (LACP)   9% at  22:17:33 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:34 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:36 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:40 Mon Feb 20, 2012
110 (ETMR)  12% at  22:17:45 Mon Feb 20, 2012
110 (ETMR)  17% at  22:17:47 Mon Feb 20, 2012
110 (ETMR)  18% at  22:17:49 Mon Feb 20, 2012
110 (ETMR)  25% at  22:20:28 Mon Feb 20, 2012
110 (ETMR)  26% at  22:39:08 Mon Feb 20, 2012
 37 (SNMP)  28% at  22:46:20 Mon Feb 20, 2012
 94 (PROX)  57% at  23:29:36 Mon Feb 20, 2012
 94 (PROX)  63% at  23:29:37 Mon Feb 20, 2012
 94 (PROX)  63% at  23:29:39 Mon Feb 20, 2012
 58 (I2C )  64% at  16:21:54 Tue Feb 21, 2012
  5 (CONS)  86% at  18:41:54 Tue Feb 21, 2012
 58 (I2C )  88% at  18:41:55 Tue Feb 21, 2012
 58 (I2C )  88% at  21:29:41 Sat Feb 25, 2012
 58 (I2C )  98% at  12:04:59 Tue Feb 28, 2012
 58 (I2C ) 100% at  11:31:32 Sat Mar 10, 2012
-----------------------------------------
```

/stats/acl
ACL Statistics Menu

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

ACL statistics are described in the following table.

Table 120. 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 196.
`acl6` *<ACL number>* Displays the IPv6 Access Control List Statistics for a specific ACL.

Table 120. ACL Statistics Menu Options (/stats/acl)

Command Syntax and Usage
`dump` Displays all ACL statistics.
`vmap` *<VMAP number>* Displays the VLAN Map statistics for a specific VMAP. For details, see page 196.
`clracl` Clears all ACL statistics.
`clracl6` Clears all IPv6 ACL 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/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 121. 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.

Table 121. SNMP Statistics (/stats/snmp) (continued)

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

Table 121. SNMP Statistics (/stats/snmp) (continued)

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

Table 121. SNMP Statistics (/stats/snmp) (continued)

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

/stats/ntp
NTP Statistics

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

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

Table 122. 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.

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 644. 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
     stack    - Stacking Menu
     qos      - QOS Menu
     acl      - Access Control List Menu
     pmirr    - Port Mirroring Menu
     l2       - Layer 2 Menu
     l3       - Layer 3 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/TFTP server
     gtcfg    - Restore current configuration from FTP/TFTP server
     cur      - Display current configuration
```

Each configuration option is briefly described in Table 123, with pointers to detailed menu commands.

Table 123. Configuration Menu Options (/cfg)

Command Syntax and Usage
`sys` Displays the System Configuration Menu. To view menu options, see page 207.
`port` *<port alias or number>* Displays the Port Configuration Menu. To view menu options, see page 244.
`stack` Displays the Stacking Configuration Menu. This menu is visible only if stacking is enabled from the `/boot` menu, and the switch is reset. To view menu options, see page 253. **Note:** This option only appears if you have stacking turned on.
`qos` Displays the Quality of Service Configuration Menu. To view menu options, see page 255.
`acl` Displays the ACL Configuration Menu. To view menu options, see page 261.

Table 123. Configuration Menu Options (/cfg) (continued)

Command Syntax and Usage
`pmirr` Displays the Mirroring Configuration Menu. To view menu options, see page 279.
`l2` Displays the Layer 2 Configuration Menu. To view menu options, see page 281.
`l3` Displays the Layer 3 Configuration Menu. To view menu options, see page 325.
`rmon` Displays the Remote Monitoring (RMON) Configuration Menu. To view menu options, see page 429.
`virt` Displays the Virtualization Configuration Menu. To view menu options, see page 434.
`dump` Dumps current configuration to a script file. For details, see page 448.
`ptcfg` *<FTP/TFTP server host name or IP address> <filename on host>* Backs up current configuration to FTP/TFTP server. For details, see page 448.
`gtcfg` *<host name or IP address of FTP/TFTP server> <filename on host>* Restores current configuration from FTP/TFTP server. For details, see page 449.
`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 1/10Gb Uplink ESM (GbESM).

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 474.

/cfg/sys
System Configuration Menu

```
[System Menu]
     linevty  - Lines Telnet SSH Menu
     linecons - Lines Console 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
     linkscan - Set linkscan mode
     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
     pktlog   - Enable/disable CPU packet logging capability
     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 124. System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`linevty` Configures the number of lines per screen displayed in the CLI by default for Telnet and SSH sessions.
`linecons` Configures the number of lines per screen displayed in the CLI by default for console sessions.
`errdis` Displays the Error Disable Recovery menu. To view menu options, see page 210.
`syslog` Displays the Syslog Menu. To view menu options, see page 211.
`sshd` Displays the SSH Server Menu. To view menu options, see page 213.

Table 124. System Configuration Menu Options (/cfg/sys) (continued)

Command Syntax and Usage
`radius` Displays the RADIUS Authentication Menu. To view menu options, see page 214.
`tacacs+` Displays the TACACS+ Authentication Menu. To view menu options, see page 216.
`ldap` Displays the LDAP Authentication Menu. To view menu options, see page 219.
`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 220.
`ssnmp` Displays the System SNMP Menu. To view menu options, see page 221.
`access` Displays the System Access Menu. To view menu options, see page 234.
`dst` Displays the Custom Daylight Savings Time menu. To view menu options, see page 241.
`sflow` Displays the sFlow menu. To view menu options, see page 242.
`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 Saving Time, etc.
`dlight enable|disable` Disables or enables daylight saving time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. The default value is `disabled`.

Table 124. System Configuration Menu Options (/cfg/sys) (continued)

Command Syntax and Usage
`idle` *<idle timeout in minutes>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 10 minutes.
`linkscan {fast|normal|slow}` Configures the link scan interval used to poll the status of ports.
`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.
`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`.
`pktlog disable|enable` Enables or disables logging of packets that come to the CPU. The default setting is `enabled`.
`cur` Displays the current system parameters.

/cfg/sys/linevty
Lines Per Screen in Telnet/SSH Configuration

```
[Lines Telnet SSH Menu]
     length   - Set lines-per-page 0-300, zero for infinite
```

Use this command to configure/cfg/sys/linecons
Lines Per Screen in Console Configuration

```
[Lines Console Menu]
     length   - Set lines-per-page 0-300, zero for infinite
```

User this command to configure

/cfg/sys/errdis
Error Disable Configuration

```
[System ErrDisable 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 125. Error Disable Configuration Options

Command Syntax and Usage
`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.
`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/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 syslogging of features
     buffer   - Buffer Menu
     cur      - Display current syslog settings
```

Table 126. 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 is 0.
facil2 *<syslog host local facility (0-7)>* This option sets the facility level of the second syslog host displayed. The default 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 of console output of syslog messages.

Table 126. 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 Buffer menu. To view menu options, see page 212.
`cur` Displays the current syslog settings.

/cfg/sys/syslog/buffer
Syslog Buffer Menu

```
[Buffer Menu]
     severity - Severity level of syslog messages write to flash
```

The following commands enable you to store messages of a particular severity.

Table 127. System Host Log Buffer Options

Command Syntax and Usage
`severity` *<syslog buffer severity (0–7)>* Sets the severity level of the syslog messages saved to flash memory. The default is 7, which means log all severity levels.

/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 GbESM, this menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see page 448).

Table 128. SSH Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage
`scpadm` Set the administration password for SCP access.
`hkeygen` Generate the RSA host 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 129. 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.

Table 129. RADIUS Server Configuration Menu Options (/cfg/sys/radius) (continued)

Command Syntax and Usage
`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.
`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 primary TACACS+ server hostname|IP address
     secsrv   - Set secondary TACACS+ server hostname|IP address
     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/https
     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 130. 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.

Table 130. TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

Command Syntax and Usage
`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.
`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 enable|disable` 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 GbESM, contact your IBM Service and Support line.

Table 130. TACACS+ Server Menu Options (/cfg/sys/tacacs) (continued)

Command Syntax and Usage
`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`.
`cauth enable|disable` Enables or disables TACACS+ command authorization.
`clog enable|disable` Enables or disables TACACS+ command logging.
`dreq enable|disable` 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 131. 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 GbESM, contact your Service and Support line.
`on` Enables the LDAP server.

Table 131. LDAP Server Menu Options (/cfg/sys/ldap) (continued)

Command Syntax and Usage
`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
      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 132. NTP Configuration Menu Options (/cfg/sys/ntp)

Command Syntax and Usage
`prisrv` *<IP address>* Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock.
`secsrv` *<IP address>* Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.
`intrval` *<5-44640>* Specifies the time interval, in minutes, to re-synchronize the switch clock with the NTP server.
`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/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 N/OS supports SNMP-based network management. In SNMP model of network management, a management station (client/manager) accesses a set of variables known as MIBs (Management Information Base) provided by the managed device (agent). If you are running an SNMP network management station on your network, you can manage the switch using the following standard SNMP MIBs:

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

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

SNMP parameters that can be modified include:

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

Table 133. System SNMP Menu Options (/cfg/sys/ssnmp)

Command Syntax and Usage
`snmpv3` Displays SNMPv3 menu. To view menu options, see page 223.
`name` *<1-64 characters>* Configures the name for the system.
`locn` *<1-64 characters>* Configures the name of the system location.

Table 133. 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 134. 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 225.
`view` *<vacmViewTreeFamily number (1-128)>* Allows you to create different MIB views. To view menu options, see page 226.
`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 227.
`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 229.
`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 230.

Table 134. 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 231.
`tparam` *<target parameters 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 232.
`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 233.
`v1v2 disable|enable` Allows you to enable or disable the access to SNMP version 1 and version 2. The default setting is enabled.
`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 135. 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 136. 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 137. 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.

Table 137. View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access) (continued)

Command Syntax and Usage
`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.
`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 138. 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 225.
`gname` *<1-32 characters>* The name for the access group as defined in `/cfg/sys/ssnmp/snmpv3/access/name` on page 227.
`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 139. 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 140. 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/IPv6 address that can be used in the generation of SNMP traps. IPv6 addresses are not displayed in the configuration, but they do receive 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 232.
`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 141. 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 225) 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 142. 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 143. System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage
`mgmt` Displays the Management Configuration Menu. To view menu options, see page 235.
`user` Displays the User Access Control Menu. To view menu options, see page 236.
`https` Displays the HTTPS Menu. To view menu options, see page 239.
`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. It is disabled by default.
`tnet enable|disable` Enables or disables Telnet access. This command is disabled by default.

Table 143. System Access Menu Options (/cfg/sys/access) (continued)

Command Syntax and Usage
`tsbbi enable|disable` Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).
`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 144. 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 N/OS browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address and mask address in dotted-decimal notation. **Note**: If you configure the management network without including the switch interfaces, the configuration causes the Firewall Load Balancing health checks to fail and creates a “Network Down” state on the network. 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 145. 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 237.
`eject user|oper|admin|`*<user name>* Ejects the specified user from the GbESM.
`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 GbESM, 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 145. 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 238.
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 146. 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 N/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 147. 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 148. 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 value 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. You can create a new certificate defining the information you 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. The switch will then restart the 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 or server-IP-addr> <server-filename>* Enables you to import a certificate authority root certificate using TFTP.
`gthkey` *<hostname or server-IP-addr> <server-filename>* Enables you to import a host private key using TFTP.

Table 148. HTTPS Access Configuration Menu Options (/cfg/sys/access/https) (continued)

Command Syntax and Usage
`gthcert` <*hostname or server-IP-addr*> <*server-filename*> Enables you to import a host certificate using TFTP.
`cur` Displays the current SSL Web Access configuration.

/cfg/sys/dst

Custom Daylight Saving 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 Saving Time. The DST will be defined by two rules: the start rule and the 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 149. 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.

`ena` Enables the Custom Daylight Saving Time settings.
`dis` Disables the Custom Daylight Saving 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 N/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 150. 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 151. 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 INT1 Menu]
     errdis   - ErrDisable 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
     learn    - Enable/Disable FDB Learning for port
     tag      - Enable/disable VLAN tagging for port
     tagpvid  - Enable/disable tagging on pvid
     fastfwd  - Enable/disable Port Fast Forwarding mode
     floodblk - Enable/disable Port flood blocking
     brate    - Set BroadCast Threshold
     mrate    - Set MultiCast Threshold
     drate    - Set Dest. Lookup Fail Threshold
     trust    - Set port as DHCP Snooping trusted or untrusted port
     dhrate   - Set DHCP packets rate limit for port
     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).

Table 152. Port Configuration Menu Options (/cfg/port)

Command Syntax and Usage
`errdis` Displays the Error Disable and Recovery menu. To view menu options, see page 247.
`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 248.
`udld` Displays the Unidirectional Link Detection (UDLD) Menu. To view menu options, see page 249.
`oam` Displays the OAM Discovery Configuration Menu. To view menu options, see page 250.
`aclqos` Displays the ACL/QoS Configuration Menu. To view menu options, see page 251.

Table 152. Port Configuration Menu Options (/cfg/port) (continued)

Command Syntax and Usage
`stp` Displays the Spanning Tree Port menu. To view menu options, see page 252.
`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.
`learn disable|enable` Enables or disables FDB learning on the port.
`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.
`fastfwd disable|enable` Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state. This feature permits the GbESM to interoperate well within Rapid Spanning Tree networks.
`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.

Table 152. Port Configuration Menu Options (/cfg/port) (continued)

Command Syntax and Usage
`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.
`trust disable|enable` Disables or enables the port as DHCP Snooping trusted.
`dhrate <1-2048>|dis` Limits the number of DHCP packets per second for the port to the specified value. If disabled (`dis`), the port forwards all unknown DHCP packets.
`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 247.)
`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 GbESM is reset. See the "Operations Menu" on page 451 for other operations-level commands.

/cfg/port <port alias or number>/errdis
Port Error Disable and Recovery Configuration

```
[Port 2 ErrDisable 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 153. Port Error Disable Configuration Options

Command Syntax and Usage
`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`).
`dis` Enables automatic error-recovery for the port.
`cur` Displays current port Error Disable parameters.

/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
     fastld   - Enable/disable non IEEE fast link down detection
     cur      - Display current gig link configuration
```

Link menu options are described in the following table.

Table 154. 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. Choices include: – 10 Mbps – 100 Mbps – 1000 Mbps – 10000 Mps – any (auto negotiate port speed)
`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.
`fastld e|d` Enables or disables Fast Link Down detection, which allows the switch to quickly detect link-down events on 1G copper ports (1000BASE-T). **Note**: This command applies only to 1G copper ports.
`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 155. 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 status changes to `errdisabled` 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 156. 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 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
```

Note:

Table 157. 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, but the total number of precedence levels allowed is eight. **Note**: When IPv6 ACLs are applied to a port, IPv4 ACLs are restricted to ACL 1-384.
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 INT1 STP Menu]
     edge     - Enable/disable edge port
     link     - Set port link type
     guard    - Set Port Guard Type Menu
     cur      - Display current port stp configuration
```

Table 158. 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`.
`guard` Displays the Spanning Tree Guard menu for the port. To view menu options, see page 253.
`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 159. 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/stack

Stacking Configuration Menu

```
[Stacking Menu]
     swnum    - Switch Number Menu
     name     - Set stack name
     backup   - Set backup switch number
     cur      - Display current stacking configuration
```

A *stack* is a group of switches that work together as a unified system. The network views a stack of switches as a single entity, identified by a single network IP address. Each unit can have a management interface IP configured. Configuration is allowed only from the master IP. On members, only information regarding their

own management interface IP is visible. The Stacking Configuration menu is used to configure a stack, and to define the Master and Backup interface that represents the stack on the network.

The Stacking Configuration menu is available only after Stacking is enabled and the switch is reset. For more information, see "Stacking Boot Menu" on page 465.

Table 160. Stacking Menu Options (/cfg/stack)

Command Syntax and Usage
`swnum` *<switch number (1-8)>* Displays the Stacking Switch menu. To view menu options, see page 254.
`name` *<1-63 characters>* Defines a name for the stack.
`backup` *<1-8>*`|0` Defines the backup switch in the stack, based on its configured switch number (csnum).
`cur` Displays the current stacking parameters.

/cfg/stack/swnum <1-8>
Stacking Switch Menu

```
[Switch 1 Menu]
     uuid     - Set Switch Chassis UUID
     bay      - Set Switch Bay Number
     bind     - Bind UUID/Bay to switch in stack
     del      - Delete switch
     cur      - Display current Switch configuration
```

Table 161. Stacking Switch Menu Options (/cfg/stack/swnum)

Command Syntax and Usage
`uuid` *<UUID>* Binds the selected switch to the stack, based on the UUID of the chassis in which the switch resides. You also must enter the bay number to specify a switch within the chassis. Following is an example UUID: `uuid 49407441b1a511d7b95df58f4b6f99fe`
`bay` *<1-10>* Binds the selected switch to the stack, based on its bay number in the chassis. You also must enter the UUID to specify the chassis in which the switch resides.
`bind` *<asnum (1-8)>* Binds the selected switch to the stack, based on its attached switch number (asnum).

Table 161. Stacking Switch Menu Options (/cfg/stack/swnum) (continued)

Command Syntax and Usage
`del` Deletes the selected switch from the stack.
`cur` Displays the current stacking switch parameters.

/cfg/qos
Quality of Service Configuration Menu

```
[QOS Menu]
     8021p    - 802.1p Menu
     dscp     - Dscp Menu
     advbuf   - Advanced Buffer Management 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 162. Quality of Service Menu Options (/cfg/qos)

Command Syntax and Usage
`8021p` Displays 802.1p configuration menu. To view menu options, see page 256.
`advbuf` Displays the Advanced Buffer Management menu. To view menu options, see page 257.
`dscp` Displays DSCP configuration menu. To view menu options, see page 260.
`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
     numcos   - Set number of 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 163. 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. **Note**: Priority value 7 is reserved for Stacking.
`qweight` *<COSq number> <weight (0-15)>* Configures the weight of the selected COSq. Enter the COSq number, followed by the scheduling weight (0-15). The valid range of the COSq number is set using the `numcos` command.
`numcos 2|8` Sets the number of Class of Service queues (COSq) for switch ports. Depending on the `numcos` setting, the valid COSq range for the `priq` and `qweight` commands is as follows: – If `numcos` is 2 (the default), the COSq range is 0-1. – If `numcos` is 8, the COSq range is 0-7. You must apply, save, and reset the switch to activate the new configuration. **Note**: In Stacking mode, the number of COS queues available is 1 or 7, because one COS queue is reserved for Stacking.
`cur` Displays the current 802.1p parameters.

/cfg/qos/advbuf
Advanced Buffer Management Menu

```
[Advanced Buffer Management Menu]
     egress    - Egress buffer policy configuration menu
     ingress   - Ingress buffer policy configuration menu
     cur       - Display current buffer policy configuration
```

Table 164. Advanced Buffer Management Menu Options (/cfg/qos/advbuf)

Command Syntax and Usage
`egress` Displays the Egress buffer policy configuration menu. To view menu options, see page 257.
`ingress` Displays the Ingress buffer policy configuration menu. To view menu options, see page 258.
`cur` Displays the current buffer policy parameters.

/cfg/qos/advbuf/egress
Egress Buffer Policy Configuration Menu

```
[Egress Buffer Menu]
     eport     - Egress buffer configuration for port(s) menu
     totcell   - Congigure total shared cell in Kbytes
     showe     - Show egress buffer configuration for port(s)
     default   - Default all egress buffer management parameters
```

Table 165. Egress Buffer Management Menu Options (/cfg/qos/advbuf/egress)

Command Syntax and Usage
`eport` *<port number>* Displays the Egress buffer configuration for ports menu. To view menu options, see page 258.
`totcell` *<total shared cell (0-2047)> <reset value (0-4)>* Configures the total shared cell in Kbytes. To use the default configuration for a field, enter “0”.
`showe` <**all**|**diff**|*port number*|*range (INT1-14, MGT1-2, EXT1-9)*> Displays the egress buffer configuration for the specified ports.
`default` Sets all egress buffer policy parameters to default values.

/cfg/qos/advbuf/egress/eport *<1-25>*

Egress Port Buffer Policy Configuration Menu

```
[Egress Port Buffer Menu]
     pkt      - Configure packet limit per queue
     cell     - Configure cell limit per queue in Kbytes
     pshare   - Configure the shared cell by all Qs per egress port in Kbytes
     cur      - Display current egress buffer policy configuration
```

Table 166. Egress Port Buffer Policy Configuration Options (/cfg/qos/advbuf/egress/eport)

Command Syntax and Usage
`pkt` *<pkt limit (0-2048)> <reset value (0-4)> <queue (1-2)>* Sets the packet limit per queue. To use the default configuration for a field, enter "0".
`cell` *<cell limit (0-2047)> <reset value (0-4)> <queue (1-2)>* Sets the cell limit per queue in Kbytes. To use the default configuration for a field, enter "0".
`pshare` *<cell limit (4-2047)> <reset value (0-4)>* Sets the shared cell by all queues per egress port in Kbytes. To use the default configuration for a field, enter "0".
`cur` Displays the current egress buffer management parameters.

/cfg/qos/advbuf/ingress

Ingress Buffer Policy Configuration Menu

```
[Ingress Buffer Menu]
     iport    - Ingress buffer configuration for port(s) menu
     showi    - Show egress buffer configuration for port(s)
     default  - Default all ingress buffer management parameters
```

Table 167. Ingress Buffer Management Menu Options (/cfg/qos/advbuf/ingress)

Command Syntax and Usage
`iport` Displays the Ingress buffer configuration for port(s) menu. To view menu options, see page 259.
`showi` <**all**|**diff**|*port number*|*range (INT1-14, MGT1-2, EXT1-9)*> Displays the ingress buffer configuration for the specified ports.
`default` Sets all egress buffer policy parameters to default values.

/cfg/qos/advbuf/ingress/iport <1-25>

Ingress Port Buffer Policy Configuration Menu

```
[Ingress Port Buffer Menu]
     pkt      - Configure flow control packet limit
     cell     - Configure flow control cell limit
     discard  - Configure flow control cell discard limit
     cur      - Display current ingress buffer policy configuration
```

Table 168. Ingress Port Buffer Policy Configuration Options (/cfg/qos/advbuf/ingress/iport)

Command Syntax and Usage
`pkt` *<pkt limit (0-8191)> <reset value (0-4)>* Sets the flow control packet limit. To use the default configuration for a field, enter “0”.
`cell` *<cell limit (0-1023)> <reset value (0-4)>* Sets the flow control cell limit in Kbytes. To use the default configuration for a field, enter “0”.
`discard` *<cell limit (4-1023)>* Sets the discard cell limit in Kbytes. To use the default configuration for a field, enter “0”.
`cur` Displays the current ingress buffer management 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 169. 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
     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 251.

Table 170. ACL Menu Options (/cfg/acl)

Command Syntax and Usage
`acl` *<1-640>* Displays Access Control List configuration menu. To view menu options, see page 262.
`acl6` *<1-128>* Displays Access Control List configuration menu. To view menu options, see page 272.
`group` *<1-640>* Displays ACL group configuration menu. To view menu options, see page 277.
`vmap` *<1-128>* Displays ACL VLAN Map configuration menu. To view menu options, see page 278.
`cur` Displays the current ACL parameters.

/cfg/acl/acl <*ACL number*>
ACL Configuration Menu

```
[ACL 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 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 171. ACL Menu Options (/cfg/acl/acl x)

Command Syntax and Usage
`mirror` Displays the ACL Port Mirror menu. To view menu options, see page 263.
`ethernet` Displays the ACL Ethernet Header menu. To view menu options, see page 264.
`ipv4` Displays the ACL IP Header menu. To view menu options, see page 265.
`tcpudp` Displays the ACL TCP/UDP Header menu. To view menu options, see page 266.
`meter` Displays the ACL Metering menu. To view menu options, see page 267.
`re-mark` Displays the ACL Re-Mark menu. To view menu options, see page 268.
`pktfmt` *<packet format>* Displays the ACL Packet Format menu. To view menu options, see page 271.
`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.

Table 171. ACL Menu Options (/cfg/acl/acl x) (continued)

Command Syntax and Usage
`reset` Resets the ACL parameters to their default values.
`cur` Displays the current ACL parameters.

/cfg/acl/acl <*ACL number*>/mirror
ACL Mirroring Configuration

```
[Mirror Options Menu]
     dest     - Set mirror destination
     port     - Set port as mirror target
     del      - Clear mirror settings
     cur      - Display current mirror configuration
```

This menu allows you to define port mirroring for an ACL. Packets that match the ACL are mirrored to the destination interface.

Table 172. ACL Port Mirroring Options

Command Syntax and Usage
`dest port|none` Configures the interface type of the destination.
`port` *<port alias or number>* Configures the destination to which packets that match this ACL are mirrored.
`del` Removes this ACL from port mirroring.
`cur` Displays the current port mirroring parameters for the ACL.

/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 173. 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 174. 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 175. 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
     log      - Enable syslog/traps when rate exceeded
     cur      - Display current settings
```

This menu defines the metering profile for the selected ACL.

Table 176. ACL Metering Menu Options (/cfg/acl/acl x/meter)

Command Syntax and Usage
`cir` <*64-10000000*> 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` Resets ACL metering parameters to their default values.
`log e|d` Enables or disables syslog notification messages for packets that do not conform to the ACL profile.
`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 177. 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 269.
`outprof` Displays the Re-Mark Out-of-Profile menu. To view menu options, see page 270.
`up1p` Displays the Re-Mark Update User Priority menu. To view menu options, see page 270.
`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 178. 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 270.
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 179. 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/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 180. 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 181. 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
```

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

Table 182. IPv6 ACL Options

Command Syntax and Usage
`ipv6` Displays the ACL IP Header menu. To view menu options, see page 273.
`tcpudp` Displays the ACL TCP/UDP Header menu. To view menu options, see page 274.
`re-mark` Displays the ACL Re-Mark menu. To view menu options, see page 275.
`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 183. 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 184. 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 185. IPv6 ACL Re-Mark Options

Command Syntax and Usage
`inprof` Displays the Re-Mark In-Profile menu. To view menu options, see page 275.
`up1p` Displays the Update User Priority menu. To view menu options, see page 276.
`reset` Reset ACL re-mark parameters to their default values.
`cur` Displays current re-mark parameters.

/cfg/acl/acl6 <*ACL number*>/re-mark/inprof
IPv6 Re-Marking In-Profile Configuration

```
[Re-marking - In Profile Menu]
     updscp   - Set the update DSCP
     reset    - Reset update DSCP settings
     cur      - Display current settings
```

Table 186. IPv6 ACL Re-Mark In-Profile Options

Command Syntax and Usage
`updscp` *<0-63>* Re-marks the DiffServ Code Point (DSCP) of in-profile packets to the selected value.
`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/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 187. 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/group <*ACL group number*>
ACL Group Configuration Menu

```
[ACL Group 1 Menu]
     add      - Add ACL to group
     rem      - Remove ACL from group
     add6     - Add IPv6 ACL to ACL group
     rem6     - Remove IPv6 ACL from ACL 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 188. ACL Group Menu Options (/cfg/acl/group x)

Command Syntax and Usage
`add acl` *<1-640>* Adds the selected ACL to the ACL group.
`rem acl` *<1-640>* Removes the selected ACL from the ACL group.
`add6` *<1-128>* Adds the selected IPv6 ACL to the ACL group.
`rem6` *<1-128>* Removes the selected IPv6 ACL from the ACL group.
`cur` Displays the current ACL group 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 261.

For more information about assigning VLAN Maps to a VLAN, see "VLAN Configuration Menu" on page 320.

For more information about assigning VLAN Maps to a VM group, see "VM Group Configuration" on page 439.

/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 GbESM, see “Appendix A: Troubleshooting” in the *IBM N/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 189. 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 280.
`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 190. 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
     amp      - Active Multipath Menu
     mrst     - Multiple Spanning Tree/Rapid Spanning Tree Menu
     nostp    - Disable Spanning Tree
     stg      - Spanning Tree Menu
     fdb      - FDB Menu
     lldp     - LLDP Menu
     trunk    - Trunk Group Menu
     thash    - Trunk Hash 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 191. Layer 2 Configuration Menu (/cfg/l2)

Command Syntax and Usage
`8021x` Displays the 802.1X Configuration Menu. To view menu options, see page 283.
`amp` Displays the Active MultiPath Protocol (AMP) Configuration menu. To view menu options, see page 289.
`mrst` Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu. To view menu options, see page 293.
`nostp enable|disable` When enabled, globally turns Spanning Tree `off`. All ports are placed into forwarding state. Any BPDUs 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 297.
`fdb` Displays the Forwarding Database Menu. To view menu options, see page 300.
`lldp` Displays the LLDP Menu. To view menu options, see page 303.

Table 191. 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 307.
`thash` Displays the Trunk Hash Menu. To view menu options, see page 308.
`lacp` Displays the Link Aggregation Control Protocol Menu. To view menu options, see page 310.
`failovr` Displays the Failover Configuration Menu. To view menu options, see page 312.
`hotlink` Displays the Hot Links Configuration menu. To view menu options, see page 317.
`vlan` *<VLAN number (1-4095)>* Displays the VLAN Configuration Menu. To view menu options, see page 320.
`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.
`macnotif enable|disable` Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.
`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 GbESM as an IEEE 802.1X Authenticator, to provide port-based network access control.

Table 192. 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 284.
`port` *<port alias or number>* Displays the 802.1X Port Menu. To view menu options, see page 287.
`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 GbESM.

Table 193. 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 286.
`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 193. 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 194. 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 GbESM. These settings override the global 802.1X parameters.

Table 195. 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 195. 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/amp

Active MultiPath Protocol Configuration

```
[Active Multipath Menu]
     group    - Active Multipath Group Configuration Menu
     agglacp  - Set active multipath aggregator LACP trunk
     aggport  - Set active multipath aggregator port
     aggtrk   - Set active multipath aggregator static trunk
     interval - Set active multipath packet interval
     priority - Set active multipath switch priority
     timeout  - Set active multipath timeout count to detect unhealthy links
     type     - Set active multipath switch type
     on       - Globally turn active multipath ON
     off      - Globally turn active multipath OFF
     default  - Default active multipath parameters
     cur      - Display current active multipath configuration
```

Use the following commands to configure Active Multipath (AMP) for the GbESM.

Table 196. AMP Configuration Options

Command Syntax and Usage
`group` *<1-22>* Displays the AMP group menu. To view menu options, see page 291.
`agglacp` *<1-65535>* | `0` Configures an LACP *admin key* to be used as the AMP Aggregator link. LACP trunks formed with this *admin key* will be used to link the two AMP Aggregators. Enter 0 (zero) to clear the Aggregator link. **Note**: This command does not apply to AMP Access switches.
`aggport` *<port alias or number>* | `0` Configures a port to be used as the AMP Aggregator link. Enter 0 (zero) to clear the Aggregator link. **Note**: This command does not apply to AMP Access switches.
`aggtrk` *<trunk number>* | `0` Configures a trunk to be used as the AMP Aggregator link. Enter 0 (zero) to clear the Aggregator link. **Note**: This command does not apply to AMP Access switches.
`interval` *<10-10000>* Configures the time interval between AMP *keep alive* messages, in centiseconds. The default value is 50.
`priority` *<1-255>* Configures the AMP priority for the switch. The default value is 255. A lower priority value denotes a higher precedence (so priority 1 is the highest priority.) It is recommended that aggregator switches be configured with lower priority values than access switches.

Table 196. AMP Configuration Options (continued)

Command Syntax and Usage
`timeout` *<1-20>* Configures the timeout count, which is the number of unreceived keep-alive packets the switch waits before declaring a timeout due to loss of connectivity with the peer. The default value is 4.
`type access|aggregator` Defines the AMP switch type, as follows: – **Access**: Connects to downstream servers. Only one AMP group can be configured on an access switch. – **Aggregator**: Connects to upstream routers. Multiple AMP groups can be configured on an Aggregator switch. The default switch type is `access`. **Note**: It is recommended to configure the 1/10Gb Uplink ESM only as an access switch.
`on` Globally turns Active MultiPath on.
`off` Globally turns Active MultiPath off.
`default` Resets Active MultiPath parameters to their default values, and optionally delete all AMP groups.
`cur` Displays the current AMP parameters.

/cfg/l2/amp/group <1-22>

AMP Group Configuration

```
[AMP Group 1 Menu]
     port     - Add port to AMP group
     port2    - Add second port to AMP group
     lacp     - Add LACP trunk to AMP group
     lacp2    - Add second LACP trunk to AMP group
     trunk    - Add static trunk to AMP group
     trunk2   - Add second static trunk to AMP group
     ena      - Enable AMP group
     dis      - Disable AMP group
     del      - Delete AMP group
     cur      - Display current AMP group configuration
```

Use the following commands to configure an AMP group.

Table 197. AMP Group Configuration Options

Command Syntax and Usage
`port` *<port alias or number>* | `0` Adds the port as the first port in the AMP group. Enter 0 (zero) to clear the port.
`port2` *<port alias or number>* | `0` Adds the port as the second port in the AMP group. Enter 0 (zero) to clear the port.
`lacp` *<1-65535>* | `0` Adds the first LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication. Enter 0 (zero) to clear the *admin key*.
`lacp2` *<1-65535>* | `0` Adds the second LACP *admin key* to the AMP group. LACP trunks formed with this *admin key* will be used for AMP communication. Enter 0 (zero) to clear the *admin key*.
`trunk` *<trunk number>* | `0` Adds the first trunk group to the AMP group. Enter 0 (zero) to clear the trunk group.
`trunk2` *<trunk number>* | `0` Adds the second trunk group to the AMP group. Enter 0 (zero) to clear the trunk group.
`ena` Enables the AMP group.
`dis` Disables the AMP group.

Table 197. AMP Group Configuration Options (continued)

Command Syntax and Usage
`del` Deletes the AMP group.
`cur` Displays the current AMP group configuration.

/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 N/OS supports STP/PVST+, 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. MSTP 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 198. 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 294.
`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 revision number for the MSTP region. The revision is used as a numerical identifier for the region. All devices within a MSTP region must have the same revision number.
`maxhop` *<4-60>* Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default is 20.
`mode mstp|rstp|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 199 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 199. CIST Menu Options (/cfg/l2/mrst/cist)

Command Syntax and Usage
`brg` Displays the CIST Bridge Menu. To view menu options, see page 295.
`port` *<port alias or number>* Displays the CIST Port Menu. To view menu options, see page 296.
`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 200. 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 INT1 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 201. 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 (for MSTP only).
`on` Enables MSTP CIST on the port.
`off` Disables MSTP CIST 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 N/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 128 is reserved for management).

Note: When VRRP is used for active/active redundancy, STG must be turned on.

Table 202. Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage
`brg` Displays the Bridge Spanning Tree Menu. To view menu options, see page 298.
`port` <*port alias or number*> Displays the Spanning Tree Port Menu. To view menu options, see page 299.
`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.
`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 203. 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 a 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 294).
`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 294).
`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 294).
`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 INT1 Menu]
     prior    - Set port Priority (0-240)
     cost     - Set port Path Cost (1-200000000 (PVRST/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 252.

Table 204. 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...). **Note**: In Stacking mode, the range is 0-255, in steps of 4 (0, 4, 8, 12...).
`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 GbESM.

Table 205. FDB Menu Options (/cfg/l2/fdb)

Command Syntax and Usage
`mcast` Displays the static Multicast menu. To view menu options, see page 301.
`static` Displays the static FDB menu. To view menu options, see page 302.
`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 206. 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` *<0-65535>*} 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` {`mac` *<MAC address>*|`vlan` *<VLAN number>*| `port` *<port alias or number>*|`all`} 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 207. 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.
`clear` *<MAC address>*|`all` {`mac`|`vlan`|`port`} Clears static FDB entries.
`cur` Display current static FDB 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 208. 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 304.
`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 208. 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 209. 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 305.
`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
     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 210. 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.
`macphy d|e` Enables or disables the MAC/Phy Configuration information type.

Table 210. Optional TLV Menu Options (/cfg/l2/lldp/port x/tlv) (continued)

Command Syntax and Usage
`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.
`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 GbESMs 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 16 trunk groups can be configured on the GbESM, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to 8 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-IBM devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 211. 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]
     set      - Trunk Hash Settings Menu
     ingress  - Enable/disable ingress port hash
     L4port   - Enable/disble L4 port hash
     localprf - Enable/disble dmlt local preference
     cur      - Display current Trunk Hash configuration
```

Use the following commands to configure IP trunk hash settings for the GbESM. Trunk hash parameters are set globally for the GbESM. 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 212 combined with the hash parameters listed in Table 213.

Table 212. Trunk Hash Settings (/cfg/l2/thash)

Command Syntax and Usage
`set` Displays the Trunk Hash Settings menu. To view menu options, see page 309.
`ingress enable|disable` Enables or disables trunk hash computation based on the ingress port. The default setting is `disabled`.
`L4port enable|disable` Enables or disables use of Layer 4 service ports (TCP, UDP, and so on) to compute the hash value. The default setting is `disable`.
`localprf enable|disable` Enables or disables Distributed Multi-Link Trunking (DMLT) local preference for the stack. The default setting is `disable`.
`cur` Display current trunk hash configuration.

/cfg/l2/thash/set

Trunk Hash Settings

```
[set Trunk Hash Settings Menu]
     smac     - Enable/disable smac hash
     dmac     - Enable/disable dmac hash
     sip      - Enable/disable sip hash
     dip      - Enable/disable dip hash
     cur      - Display current trunk hash setting
```

You can enable one or two of the following parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

Use the following commands to configure IP trunk hash parameters for the GbESM.

Table 213. Trunk Hash Parameters (/cfg/l2/thash/set)

Command Syntax and Usage
`smac enable|disable` Enable or disable trunk hashing on the source MAC.
`dmac enable|disable` Enable or disable trunk hashing on the destination MAC.
`sip enable|disable` Enable or disable trunk hashing on the source IP.
`dip enable|disable` Enable or disable trunk hashing on the destination IP.
`cur` Display current trunk hash settings.

/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 GbESM.

Table 214. 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 311.
`sysprio` *<1-65535>* Defines the priority value (1 through 65535) for the GbESM. 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 GbESM'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*.
`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 215. 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` <*1-8*> 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.
`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 N/OS Application Guide*.

Table 216. 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 313.
`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 217. 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 314.
mmon Displays the Manual Monitor menu for the selected trigger. To view menu options, see page 314.
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 218. 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 let you manually define both the monitor and control ports that participate in failover teaming.

Note: AMON and MMON configurations are mutually exclusive.

Table 219. Failover Manual Monitor options (/cfg/l2/failovr/trigger/mmon)

Command Syntax and Usage
monitor Displays the Manual Monitor - Monitor menu for the selected trigger.
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 220. 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 221. Failover Manual Monitor Control Options (/cfg/l2/failovr/trigger/mmon/control)

Command Syntax and Usage
`addport` *<port alias or number>* Adds the specified port or ports to the Manual Monitor Control configuration.
`remport` *<port alias or number>* Removes the specified port or ports 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 222 describes the Hot Links menu options.

Table 222. Hot Links Menu Options (/cfg/l2/hotlink)

Command Syntax and Usage
`trigger` *<1-200>* Displays the Hot Links Trigger menu. To view menu options, see page 318.
`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` *<10-200>* 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 <1-200>

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 223. 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 319.
`backup` Displays the Backup interface menu for the selected trigger. To view menu options, see page 319.
`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 <1-200>/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 224. 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 <*0-65535*> Adds an LACP *admin key* to the Master interface. LACP trunks formed with this *admin key* are 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 <1-200>/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 225. 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.
adminkey <*0-65535*> Adds an LACP *admin key* to the Backup interface. LACP trunks formed with this *admin key* are 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 1024 VLANs can be configured on the GbESM.

VLANs can be assigned any number between 1 and 4094. VLAN 4095 is reserved for switch management.

Table 226. 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 322.
`privlan` Displays the Private VLAN menu. To view menu options, see page 324.
`name` Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.
`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.

Table 226. VLAN Configuration Menu Options (/cfg/l2/vlan) (continued)

Command Syntax and Usage
`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 (MGT1 and MGT2) 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 244).

/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 227. 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 227. 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 228. 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
     dhcp     - DHCP Configuration Menu
     cur      - Display current IP configuration
```

Table 229. 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 328.
`gw` *<default gateway number (1-4)>* Displays the IP Default Gateway Menu. To view menu options, see page 332.
`route` Displays the IP Static Route Menu. To view menu options, see page 333.
`mroute` Displays the Static IP Multicast Route Menu. To view menu options, see page 335.
`arp` Displays the Address Resolution Protocol Menu. To view menu options, see page 336.

Table 229. Layer 3 Configuration Menu (/cfg/l3) (continued)

Command Syntax and Usage
`frwd` Displays the IP Forwarding Menu. To view menu options, see page 338.
`nwf` *<network filter number (1-256)>* Displays the Network Filter Configuration Menu. To view menu options see page 339.
`rmap` *<route map number (1-32)>* Displays the Route Map Menu. To view menu options see page 340.
`rip` Displays the Routing Interface Protocol Menu. To view menu options, see page 344.
`ospf` Displays the OSPF Menu. To view menu options, see page 348.
`bgp` Displays the Border Gateway Protocol Menu. To view menu options, see page 359.
`mld` Displays the Multicast Listener Discovery Menu. To view menu options, see page 365.
`igmp` Displays the IGMP Menu. To view menu options, see page 367.
`ikev2` Displays the IKEv2 Menu. To view menu options, see page 377.
`ipsec` Displays the IPsec Menu. To view menu options, see page 380.
`dns` Displays the IP Domain Name System Menu. To view menu options, see page 390.
`bootp` Displays the Bootstrap Protocol Menu. To view menu options, see page 391.
`vrrp` Displays the Virtual Router Redundancy Configuration Menu. To view menu options, see page 395.
`gw6` *<gateway number (1, 132)>* Displays the IPv6 Gateway Configuration Menu. To view menu options, see page 405.

Table 229. Layer 3 Configuration Menu (/cfg/l3) (continued)

Command Syntax and Usage
`route6` Displays the IPv6 Routing Configuration Menu. To view menu options, see page 406.
`nbrcache` Displays the IPv6 Neighbor Discovery Cache Configuration Menu. To view menu options, see page 407.
`ip6pmtu` Displays the IPv6 Path MTU menu. To view menu options, see page 408.
`ospf3` Displays the OSPFv3 Configuration Menu. To view menu options, see page 409.
`ndprefix` Displays the IPv6 Neighbor Discovery Prefix menu. To view menu options, see page 421.
`ppt` Displays the Prefix Policy Table menu. To view menu options, see page 424.
`loopif` Displays the IP Loopback Interface Menu. To view menu options, see page 425.
`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 426.
`dhcp` Displays the DHCP Configuration Menu. To view menu options, see page 426.
`cur` Displays the current IP configuration.

/cfg/l3/if <*interface number*>
IP Interface Configuration Menu

```
[IP Interface 1 Menu]
     ip6nd    - IP6 Neighbor Discovery Menu
     addr     - Set IP address
     secaddr6 - Set Secondary IPv6 address on IPv6 interface
     maskplen - Set subnet mask/prefix len
     vlan     - Set VLAN number
     relay    - Enable/disable BOOTP relay
     ip6host  - Enable/disable IPv6 host mode
     ip6dstun - Enable/disable ICMPv6 destination unreachable messages
     ena      - Enable IP interface
     dis      - Disable IP interface
     del      - Delete IP interface
     cur      - Display current interface configuration
```

The GbESM can be configured with up to 128 IP interfaces. Each IP interface represents the GbESM on an IP subnet on your network. The Interface option is disabled by default.

Note: To maintain connectivity between the management module and the GbESM, use the management module interface to change the IP address of the switch.

Table 230. IP Interface Menu Options (/cfg/l3/if)

Command Syntax and Usage
`ip6nd` Displays the IPv6 Neighbor Discovery menu. To view menu options, see page 330.
`addr` *<IPv4 address (such as 192.4.17.101)>* **IPv4:** Configures the IPv4 address of the switch interface, using dotted decimal notation. `addr` *<IPv6 address (such as 3001:0:0:0:0:0:abcd:12)>* `[anycast]` **IPv6**: Configures the IPv6 address of the switch interface, using hexadecimal format with colons.
`secaddr6` *<IPv6 address (such as 3001:0:0:0:0:0:abcd:12)>|<prefix length>* `[anycast]` Configures the secondary IPv6 address of the switch interface, using hexadecimal format with colons.
`maskplen` *<IPv4 subnet mask (such as 255.255.255.0)>* **IPv4**: Configures the IPv4 subnet address mask for the interface, using dotted decimal notation. `maskplen` *<IPv6 prefix length (1-128)>* **IPv6**: Configures the subnet IPv6 prefix length. The default value is 0 (zero).

Table 230. IP Interface Menu Options (/cfg/l3/if) (continued)

Command Syntax and Usage
`vlan <VLAN number>` Configures the VLAN number for this interface. Each interface can belong to only one VLAN. **IPv4**: Each VLAN can contain multiple IPv4 interfaces. **IPv6**: Each VLAN can contain only one IPv6 interface.
`relay disable|enable` Enables or disables the BOOTP relay on this interface. The default setting is `enabled`.
`ip6host enable|disable` Enables or disables the IPv6 Host Mode on this interface. The default setting is `disabled` for data interfaces, and `enabled` for the management interface.
`ip6dstun enable|disable` Enables or disables sending of ICMP Unreachable messages. 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/if <*interface number*>/ip6nd

IPv6 Neighbor Discovery Configuration Menu

```
[IP6 Neighbor Discovery Menu]
     rtradv   - Enable/disable router advertisement
     managed  - Enable/disable Managed config flag
     othercfg - Enable/disable Other config flag
     ralife   - Set Router Advertisement lifetime
     dad      - Set number of duplicate address detection attempts
     reachtm  - Set advertised reachability time
     advint   - Set Router Advertisement maximum interval
     advmint  - Set Router Advertisement minimum interval
     retimer  - Set Router Advertisement Retrans Timer
     hoplmt   - Set Router Advertisement Hop Limit
     advmtu   - Enable/disable Advertise MTU option
     cur      - Display current Neighbor Discovery configuration
```

Table 231 describes the IPv6 Neighbor Discovery configuration options.

Table 231. IPv6 Neighbor Discovery Options

Command Syntax and Usage
`rtradv e|d` Enables or disables IPv6 Router Advertisements on the interface. The default value is `disabled`.
`managed e|d` Enables or disables the *managed address configuration* flag of the interface. When enabled, the host IP address can be set automatically through DHCP. The default value is `disabled`.
`othercfg e|d` Enables or disables the *other stateful configuration* flag, which allows the interface to use DHCP for other stateful configuration. The default value is `disabled`.
`ralife` <*0-9000*> Configures the IPv6 Router Advertisement lifetime interval. The RA lifetime interval must be greater than or equal to the RA maximum interval (`advint`), or 0 (zero). The default value is 1800 seconds.
`dad` <*1-10*> Configures the maximum number of duplicate address detection attempts. The default value is 1.
`reachtm` <*0-3600*> `reachtm` <*0-3600000*> `ms` Configures the advertised reachability time, in seconds or milliseconds (ms). The default value is 30 seconds.

Table 231. IPv6 Neighbor Discovery Options

Command Syntax and Usage
`advint` *<4-1800>* Configures the Router Advertisement maximum interval. The default value is 600 seconds. **Note**: Set the maximum RA interval to a value greater than or equal to 4/3 of the minimum RA interval.
`advmint` *<3-1800>* Configures the Router Advertisement minimum interval. The default value is 198 seconds. **Note**: Set the minimum RA interval to a value less than or equal to 0.75 of the maximum RA interval.
`retimer` *<0-4294967>* `retimer` *<0-4294967295>* `ms` Configures the Router Advertisement re-transmit timer, in seconds or milliseconds (ms). The default value is 1 second.
`hoplmt` *<0-255>* Configures the Router Advertisement hop limit. The default value is 64.
`advmtu e|d` Enables or disables the MTU option in Router Advertisements. The default setting is `enabled`.
`cur` Displays the current Neighbor Discovery parameters.

/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. Gateway 4 is reserved for switch management.

This option is disabled by default.

Table 232. 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 Menu2

```
[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
     bgptoecmp - Enable/disable BGP to ECMP functionality
     cur      - Display current static routes
```

Up to 128 IPv4 static routes can be configured.

Table 233. 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

Table 233. IP Static Route Configuration Menu Options (cfg/l3/route) (continued)

Command Syntax and Usage
`bgptoecmp enable|disable` Enables or disables BGP to ECMP route selection. When enabled, the switch checks new BGP routes to see if there is an ECMP route with the same gateway as the new route. If one such route exists, then the switch adds a new ECMP route with the same paths but with the new destination. When a new BGP route has the next hop in one of the subnets to which an ECMP static route exists, the switch adds that BGP route as a static ECMP route.
`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 either IGMP Relay or IGMP Snooping (`/cfg/l3/igmp/snoop/ena`) must be enabled (`/cfg/l3/igmp/relay/ena`).

Table 234. 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. If IGMP Relay is enabled, indicate whether the static mroute is a primary, backup or host multicast route.
`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. If IGMP Relay is enabled, indicate whether the static mroute is a primary, backup or host multicast route.
`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. If IGMP Relay is enabled, indicate whether the static mroute is a primary, backup or host multicast route.

Table 234. IPMC Route Configuration Options

Command Syntax and Usage
`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 235. ARP Configuration Menu Options (/cfg/l3/arp)

Command Syntax and Usage
`static` Displays Static ARP menu. To view options, see page 337.
`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 236. 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 237. 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 GbESM. Forwarding is turned on by default.
`off` Disables IP forwarding (routing) on the GbESM.
`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 238. 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 239. 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 342.
`aspath` *<number 1-8>* Displays the Autonomous System (AS) Filter menu. For more information, see page 343.
`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 239. 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 240. 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 339 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.
`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 241. 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
     redist   - RIP Route Redistribute Menu
     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 242. RIP Menu Options (/cfg/l3/rip)

Command Syntax and Usage
`if` *<interface number>* Displays the RIP Interface menu. For more information, see page 345.
`update` *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.
`redist fixed|static|ospf|eospf|ebgp|ibgp` Displays the RIP Route Redistribution menu. For more information, see page 347.
`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 243. 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`.

Table 243. RIP Interface Menu Options (/cfg/l3/rip/if) (continued)

Command Syntax and Usage
`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.
`disable` Disables this RIP interface.
`current` Displays the current RIP configuration.

/cfg/l3/rip/redist fixed|static|ospf|eospf|ebgp|ibgp
RIP Route Redistribution Configuration Menu

```
[RIP 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
```

The following table describes the RIP Route Redistribute Menu options.

Table 244. RIP Redistribution Menu Options (/cfg/l3/rip/redist)

Command Syntax and Usage
add *<1-32>* *<1-32>*|all Adds selected routing maps to the RIP route redistribution list. To add specific route maps, enter routing map numbers, separated by a comma (,). To add all 32 route maps, type all. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem *<1-32>* *<1-32>*|all Removes the route map from the RIP route redistribution list. To remove specific route maps, enter routing map numbers, separated by a comma (,). To remove all 32 route maps, type all.
export *<1-15>*|none Exports the routes of this protocol 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 RIP route redistribute 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 245. 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 350 to view menu options.
`range` *<1-16>* Displays the summary range menu. See page 352 to view menu options.
`if` *<interface number>* Displays the OSPF interface configuration menu. See page 353 to view menu options.
`loopif` *<1-5>* Displays the OSPF loopback interface configuration menu. See page 355 to view menu options.
`virt` *<virtual link (1-3)>* Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See page 356 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 357 to view menu options.
`redist fixed|static|rip|ebgp|ibgp` Displays Route Distribution Menu. See page 358 to view menu options.

Table 245. OSPF Configuration Menu (/cfg/l3/ospf) (continued)

Command Syntax and Usage
`lsdb` *<LSDB limit (0-6144, 0 for no limit)>* Sets the link state database limit.
`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 GbESM.
`off` Disables OSPF on the GbESM.
`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 246. 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 246. 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 247. 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 GbESM.
`hide disable|enable` Hides the OSPF summary range.
`enable` Enables the OSPF summary range.
`disable` Disables the OSPF summary range.
`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 248. 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 GbESM'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.

Table 248. OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if) (continued)

Command Syntax and Usage
`key <key>|none` Sets the authentication key to clear the password.
`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 249. 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.
`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 250. 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.

Table 250. OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt) (continued)

Command Syntax and Usage
`disable` Disables OSPF virtual link.
`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 251. 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 252. 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 253. 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 N/OS implementation, the GbESM 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 254. Border Gateway Protocol Menu (/cfg/l3/bgp)

Command Syntax and Usage
`peer` *<peer number (1-16)>* 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 361.
`aggr` *<aggregate number (1-16)>* Displays the Aggregation Menu. To view menu options, see page 364.
`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.
`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
      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 255. 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 363.
`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.
`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` *<keepalive time (0, 1-21845)>* Sets the keep-alive time for the specified peer in seconds. The default value is 60.

Table 255. BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer) (continued)

Command Syntax and Usage
`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.
`disable` Disables this peer configuration.
`delete` Deletes this peer configuration.
`passwd` *<1-16 characters>*`|none` Configures the BGP peer password.
`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 256. 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.
`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 257. 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 258 describes the commands used to configure basic Multicast Listener Discovery parameters.

Table 258. MLD Menu Options (/cfg/l3/mld)

Command Syntax and Usage
`if` *<interface number>* Displays the MLD Interface Menu. To view menu options, see page 366.
`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 259 describes the commands used to configure Multicast Listener Discovery parameters for an interface.

Table 259. 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 bursting 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 259. 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
     on       - Globally turn IGMP ON
     off      - Globally turn IGMP OFF
     cur      - Display current IGMP configuration
```

Table 260 describes the commands used to configure basic IGMP parameters.

Table 260. IGMP Menu Options (/cfg/l3/igmp)

Command Syntax and Usage
`snoop` Displays the IGMP Snoop Menu. To view menu options, see page 368.
`relay` Displays the IGMP Relay Menu. To view menu options, see page 370.
`mrouter` Displays the Static Multicast Router Menu. To view menu options, see page 372.
`igmpflt` Displays the IGMP Filtering Menu. To view menu options, see page 373.
`adv` Displays the IGMP Advanced Menu. To view menu options, see page 376.
`on` Globally turns IGMP on.
`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 261 describes the commands used to configure IGMP Snooping.

Table 261. 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 369.
`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.
`rem` *<VLAN number>* Removes the selected VLAN(s) from IGMP Snooping.
`clear` Removes all VLANs from IGMP Snooping.
`ena` Enables IGMP Snooping.

Table 261. IGMP Snoop Menu Options (/cfg/l3/igmp/snoop) (continued)

Command Syntax and Usage
`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 262 describes the commands used to configure IGMP version 3.

Table 262. 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`.
`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
     cur      - Display current IGMP Relay configuration
```

Table 263 describes the commands used to configure IGMP Relay.

Table 263. 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 371.
`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.
`dis` Disables IGMP Relay.
`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 264 describes the commands used to configure the IGMP Relay multicast router.

Table 264. 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.
`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 265 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 265. 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 266 describes the commands used to configure an IGMP filter.

Table 266. 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 374.
`port` *<port alias or number>* Displays the IGMP Filtering Port Menu. To view menu options, see page 375.
`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 267 describes the commands used to define an IGMP filter.

Table 267. 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 268 describes the commands used to configure a port for IGMP filtering.

Table 268. 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 269 describes the commands used to configure advanced IGMP parameters.

Table 269. 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.
`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/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 270 describes the commands used to configure IKEv2.

Table 270. IKEv2 Menu Options (/cfg/l3/ikev2)

Command Syntax and Usage
`prop` Displays the IKEv2 Proposal Menu. To view menu options, see page 378.
`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 378.
`ident` Displays the IKEv2 Identification Menu. To view menu options, see page 379.
`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 271 describes the commands used to configure an IKEv2 proposal.

Table 271. 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 272 describes the commands used to configure an IKEv2 preshared key.

Table 272. 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 379.
`cur` Displays the current IKEv2 preshare key settings.

/cfg/l3/ikev2/psk/rem-key

IKEv2 Preshare Key Remote ID 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 273 describes the commands used to configure an IKEv2 preshared key remote ID.

Table 273. 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 274 describes the commands used to configure IKEv2 identification.

Table 274. 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.
`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 configuration
```

Table 275 describes the commands used to configure IPsec.

Table 275. IPsec Menu Options (/cfg/l3/ipsec)

Command Syntax and Usage
`txform` *<1-10>* Displays the Transform Set Menu. To view menu options, see page 381.
`selector` *<1-10>* Displays the Traffic Selector Menu. To view menu options, see page 382.
`policy` Displays the IPsec Policy Menu. To view menu options, see page 383.
`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 276 describes the commands used to configure an IPsec transform set.

Table 276. 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 277 describes the commands used to configure an IPsec traffic selector.

Table 277. 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 383.
`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 278 describes the commands used to configure IPsec protocol matching.

Table 278. 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 279 describes the commands used to configure an IPsec policy.

Table 279. 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 384.
`manual` *<1-10>* Displays the IPsec Manual Policy menu. To view menu options, see page 385.
`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 280 describes the commands used to configure an IPsec dynamic policy.

Table 280. 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 281 describes the commands used to configure an IPsec manual policy.

Table 281. 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 386.
`in-esp` Displays the Inbound ESP Session Options menu. To view menu options, see page 387.
`out-ah` Displays the Outbound AH Session Options menu. To view menu options, see page 388.
`out-esp` Displays the Outbound ESP Session Options menu. To view menu options, see page 389.
`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 282 describes the commands used to configure an IPsec manual policy inbound authentication header (AH).

Table 282. 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. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.
`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 283 describes the commands used to configure an IPsec manual policy inbound Encapsulating Security Payload (ESP) header.

Table 283. 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. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.
`auth-key` *<key code (hexadecimal)>* Sets inbound ESP authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.
`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 284 describes the commands used to configure an IPsec manual policy outbound authentication header (AH).

Table 284. 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. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 20 characters for SHA1 and 16 characters for MD5 encryption.
`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 285 describes the commands used to configure an IPsec manual policy outbound Encapsulating Security Payload (ESP) header.

Table 285. 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. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.
`auth-key` *<key code (hexadecimal)>* Sets outbound ESP authenticator key. **Note**: For manual policies, when peering with a third-party device, key lengths are fixed to 8 characters for DES and to 24 characters for 3DES and AES-CBC encryption.
`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
     reqver   - Set the IP version of DNS record to request first
     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 286. 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.
`reqver v4|v6` Configures the protocol used for the first request to the DNS server, as follows: – `v4`: IPv4 – `v6`: IPv6
`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
     option82 - BOOTP option 82 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 GbESM.

BOOTP relay is turned off by default.

Table 287. 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 392.
`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 393.
`option82` Displays the BOOTP DHCP Relay Option 82 menu, which enables you to configure a field that a DHCP server can use to assign IP addresses based on a client device's location in the network. To view menu options, see page 394.
`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 288. 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 289. 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 392.
`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/bootp/option82

BOOTP DHCP Relay Option 82 Configuration

```
[DHCP relay option 82 menu Menu]
     on       - Turn on BOOTP option 82
     off      - Turn off BOOTP option 82
     policy   - BOOTP option 82 policy
     reset    - Reset BOOTP option 82
     cur      - Display BOOTP option 82 configuration
```

This menu lets you configure use of “option 82,” a field that a DHCP server can use to assign IP addresses based on a client device’s location in the network.

Table 290. BOOTP DHCP Relay Option 82 Configuration Options

Command Syntax and Usage
`on` Turns on BOOTP option 82.
`off` Turns off BOOTP option 82.
`policy keep	drop	replace` Enables BOOTP Relay for the broadcast domain.
`reset` Resets BOOTP option 82 settings.
`cur` Displays the current BOOTP option 82 configuration.

/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 GbESMs 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 N/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 291. 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 397.
`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 400.
`if` *<interface number>* Displays the VRRP Virtual Router Interface Menu. To view menu options, see page 403.
`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 404.
`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 291. 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 292. 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 N/OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 399.
`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.
`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.

Table 292. VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr) (continued)

Command Syntax and Usage
`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 preempt another virtual router which has assumed master routing authority. This preemption 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 404).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router pre-emption option (see `preem` in Table 292 on page 397) 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 293. 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 GbESM 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 GbESMs in a hot-standby failover configuration, where only one switch is active at any time.

Table 294. 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 N/OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 402.
`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 294. 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 295. 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 296. 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 399), the priority level for the virtual router is increased by an amount defined through this menu.

Table 297. 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.
`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 399) 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.
- Gateway 132 is reserved for management.

The following table describes the IPv6 default gateway configuration options.

Table 298. 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 299. 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`: Default 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 300. 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 301. 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 302. 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 411 to view menu options.
`range` *<1-16>* Displays summary routes menu for up to 16 IP addresses. See page 413 to view menu options.
`summpref` *<1-16>* Displays the OSPFv3 summary prefix configuration menu. See page 414 to view menu options.
`if` *<interface number>* Displays the OSPFv3 interface configuration menu. See page 415 to view menu options.
`virt` *<virtual link (1-3)>* Displays the Virtual Links menu used to configure OSPFv3 for a Virtual Link. See page 417 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 418 to view menu options.

Table 302. OSPFv3 Configuration Menu (/cfg/l3/ospf3) (continued)

Command Syntax and Usage
`rdstcfg <1-128>` Displays the OSPF route redistribution entry menu. See page 419 to view menu options.
`redist connected|static` Displays route redistribution menu. See page 420 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 303. 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 303. 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 304. 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).
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 305. 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.
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
     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 306. OSPFv3 Interface Configuration Options (/cfg/l3/ospf3/if)

Command Syntax and Usage
`aindex` <*area index (0-2)*> Configures the OSPFv3 area index.
`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.
`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.

Table 306. OSPFv3 Interface Configuration Options (/cfg/l3/ospf3/if) (continued)

Command Syntax and Usage
`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/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 307. 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 308. 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 309. 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 310. 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 311. 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 312. 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 312. IPv6 Neighbor Discovery Profile Options (continued)

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 313. 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 314. 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 315. Flooding Menu Options (/cfg/l3/flooding)

Command Syntax and Usage
`vlan` *<VLAN number>* Displays the flooding configuration menu for the VLAN. See page 426 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 316. 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 IGMP Relay is enabled and none of the IGMP hosts reside on the same VLAN as the streaming server, disable IPMC flooding to ensure that the multicast data is routed to the clients.
`cpu enable|disable` Configures the switch to forward unregistered IP multicast traffic to the MP, which adds an entry in the IPMC table. The default setting is `enabled`. **Note**: If both `flood` and `cpu` are disabled, then the switch drops all unregistered IPMC traffic.
`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/l3/dhcp
Dynamic Host Configuration Protocol Configuration Menu

```
[Dynamic Host Configuration Protocol Menu]
     snooping - DHCP Snooping Configuration Menu
```

Table 317. DHCP Configuration Menu Options (/cfg/l3/dhcp)

Command Syntax and Usage
`snooping` Displays the DHCP Snooping Configuration menu. See page 427 to view menu options.

/cfg/l3/dhcp/snooping
DHCP Snooping Configuration Menu

```
[DHCP Snooping Menu]
     addvlan  - Enable DHCP snooping on the VLANs
     rmvlan   - Disable DHCP snooping on the VLANs
     addbind  - Add a static entry to DHCP Snooping binding table
     rmbind   - remove an entry from DHCP Snooping binding table
     on       - Globally turn DHCP Snooping on
     off      - Globally turn DHCP Snooping off
     option82 - Enable/Disable DHCP Snooping option82 function
     cur      - Display current DHCP Snooping configuration
```

Table 318. DHCP Snooping Configuration Menu Options (/cfg/l3/dhcp/snooping)

Command Syntax and Usage
`addvlan` *<VLAN number or range>* Enables DHCP snooping on the specified VLANs.
`rmvlan` *<VLAN number or range>* Disables DHCP snooping on the specified VLANs.
`addbind` *<MAC address> <IP address> <VLAN number> <port number> <lease time (1-4294967295)>* Adds a static entry to the DHCP snooping binding table.
`rmbind all` | `mac` *<MAC address>* | `port` *<port number>* | `vlan` *<VLAN number>* Removes an entry from the DHCP snooping binding table.
`on` Globally turns DHCP snooping on.
`off` Globally turns DHCP snooping off.

Table 318. DHCP Snooping Configuration Menu Options (/cfg/l3/dhcp/snooping)

Command Syntax and Usage
`option82 enable|disable` Enables or disables the DHCP snooping Option 82 function. The default setting is `disable`.
`cur` Displays the current DHCP snooping configuration.

/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 319 describes the Remote Monitoring (RMON) configuration menu options.

Table 319. 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 430.
`event` *<1-65535>* Displays the RMON Event Configuration menu. To view menu options, see page 431.
`alarm` *<1-65535>* Displays the RMON Alarm Configuration menu. To view menu options, see page 432.
`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 320 describes the RMON History Menu options.

Table 320. 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 321 describes the RMON Event Menu options.

Table 321. 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 322 describes the RMON Alarm Menu options.

Table 322. 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.

Table 322. RMON Alarm Menu Options (/cfg/rmon/alarm)

Command Syntax and Usage
`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]
     vmpolicy - Virtual Machines Policy 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 323 describes the general virtualization configuration options. More detailed information is available in the following sections.

Table 323. Virtualization Configuration Options (/cfg/virt)

Command Syntax and Usage
vmpolicy Displays the Virtual Machines Policy menu. To view menu options, see page 435.
vmcheck Displays the VM Check menu. To view menu options, see page 437.
vmgroup *<1-1024>* Displays the Virtual Machine Groups menu. To view menu options, see page 439.
vmprof Displays the Virtual Machine Profiles menu. To view menu options, see page 441.
vmware Displays the VMware settings menu. To view menu options, see page 443.
vmrmisc Displays the Miscellaneous VMready Configuration menu. To view menu options, see page 445.
enavmr Enables VMready.
disvmr Disables VMready.
cur Displays the current virtualization parameters.

/cfg/virt/vmpolicy
Virtual Machines Policy Configuration

```
[VM Policy Configuration Menu]
     vmbwidth -  VM Bandwidth Configuration Menu
```

Table 324 describes the Virtual Machines (VM) policy configuration options.

Table 324. 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 325 describes the bandwidth management options for the selected VM. Use these commands to limit the bandwidth used by each VM.

Table 325. VM Bandwidth Management Options (/cfg/virt/vmpolicy/vmbwidth)

Command Syntax and Usage
`txrate` <*64-10000000*> `[32|64|128|256|512|1024|2048|4096]` <*1-640*> 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.
`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/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 326 describes the the VM Check validation options used for MAC address spoof prevention.

Table 326. VM Check Options

Command Syntax and Usage
`action` Configures the actions taken when detecting MAC address spoofing. To view menu options, see page 438
`acls` *<1-640>* Configures the maximum number of ACLs that can be set up for MAC address spoofing prevention in advanced validation mode. Default value is 50.
`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 327 describes the VM Check actions available for handling MAC address spoof attempts.

Table 327. 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
   remport  - 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 328 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 328. 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 278.
`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 328. 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. Default setting is disabled. – `basic` validation ensures lightweight port-based protection by cross-checking 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.
`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 328. 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 329 describes the VM Profiles configuration options.

Table 329. 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 442.
`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 egress shaping parameters
     delete   - Delete this VM profile
     cur      - Show details of the current VM profile
```

Table 330 describes the VM Profile Edit options.

Table 330. 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 egress shaping parameters implemented in the hypervisor, as follows: – Average traffic, in Kilobits per second – Maximum burst size, in Kilobytes – Peak traffic, in Kilobits per second – Delete traffic shaping parameters
`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 331 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 331. 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 443.
`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 332 describes the VM Hello configuration options.

Table 332. 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/vmrmisc

Miscellaneous VMready Configuration

```
[Misc. VMready Configuration  Menu]
     addoui    - Add MAC OUI
     remoui    - Remove MAC OUI
     showoui   - Show all the configured MAC OUIs
     lmacena   - Treat locally administered MAC addresses as VMs
     lmacdis   - Do not treat locally administered MAC addresses as VMs
```

You can pre-configure MAC addresses as VM Organization Unique Identifiers (OUIs). These configuration commands are only available using the IBM N/OS CLI and the Miscellaneous VMready Configuration Menu. Table 331 describes the VMready configuration options.

Table 333. VMready Configuration Options

Command Syntax and Usage
`addoui` *<3 byte VM MAC OUI> <Vendor Name>* Adds a MAC OUI.
`remoui` *<3 byte VM MAC OUI>* Removes a MAC OUI.
`showoui` Displays all the configured MAC OUIs.
`lmacena` Enables the switch to treat locally administered MAC addresses as VMs.
`lmacdis` Disables the switch from treating locally administered MAC addresses as VMs.

/cfg/virt/evb/vsidb

Virtual Station Interface 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 334 describes the Virtual Station Interface Type database configuration options.

Table 334. Virtual Station Interface Type DataBase Configuration Options

Command Syntax and Usage
`managrip` *<IP address>* Sets the Virtual Station Interface DataBase manager IP address.
`port` *<1-65534>* Sets the Virtual Station Interface DataBase manager port.
`docpath` *<file path>* Sets the Virtual Station Interface DataBase document path.
`alltypes` *<URI>* Sets the Virtual Station Interface All DataBase URI.
`interval` *<5-300>* Sets the Virtual Station Interface DataBase update interval, in seconds.
`cur` Displays the current VSI type parameters.
`reset` Resets VSIDB parameters.

/cfg/virt/evb/profile

Edge Virtual Bridge 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 335 describes the Edge Virtual Bridge Profile configuration options.

Table 335. 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 profile configuration.

/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, as described on page 449.

/cfg/ptcfg <*FTP/TFTP 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 server. To start the switch configuration upload, at the `Configuration#` prompt, enter:

```
Configuration# ptcfg <FTP or TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the name of the target script configuration file.

Notes:

- The output file is formatted with line-breaks but no carriage returns and cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).
- If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified `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 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 or TFTP server> <filename> <username>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the name of the target script configuration file.

Chapter 7. 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
     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
```

The commands of the Operations Menu enable you to alter switch operational characteristics without affecting switch configuration.

Table 336. Operations Menu (/oper)

Command Syntax and Usage
`port` *<port alias or number>* Displays the Operational Port Menu. To view menu options, see page 453.
`vrrp` Displays the Operational Virtual Router Redundancy Menu. To view menu options, see page 455.
`ip` Displays the IP Operations Menu, which has one sub-menu/option, the Operational Border Gateway Protocol Menu. To view menu options, see page 455.
`prm` Displays the Protected Mode menu. To view menu options, see page 457.
`sys` Displays the Operational System menu. To view menu options, see page 458.
`virt` Displays the Virtualization Operations Menu. To view menu options, see page 458.

Table 336. Operations Menu (/oper) (continued)

Command Syntax and Usage
`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.

/oper/port <*port alias or number*>
Operations-Level Port Options Menu

```
[Operations Port INT1 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 337. Operations-Level Port Menu Options (/oper/port)

Command Syntax and Usage
`8021x` Displays the 802.1X Port Menu. To view menu options, see page 454.
`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 338. 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/vrrp
Operations-Level VRRP Options Menu

```
[VRRP Operations Menu]
       back   - Set virtual router to backup
```

Table 339. Operations-Level VRRP Menu Options (/oper/vrrp)

Command Syntax and Usage
back *<virtual router number (1-128)>* 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 340. 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 456.

/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 341. Operations-Level BGP Menu Options (/oper/ip/bgp)

Command Syntax and Usage
`start` *<peer number (1-16)>* Starts the peer session.
`stop` *<peer number (1-16)>* 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 342. 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 342. 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
```

I2C device commands are to be used only by Technical Support personnel.

/oper/virt
Virtualization Operations

```
[Virtualization Operations Menu]
     vmware   - VMware Operations Menu
```

Table 343 describes general virtualization operations options. More details are available in the following sections.

Table 343. Virtualization Options (/oper/virt)

Command Syntax and Usage
`vmware` Displays the VMware operations menu. To view the menu options, see page 459.

/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 344. VMware Operations (/oper/virt/vmware)

Command Syntax and Usage
`dvswitch` Displays the VMware Distributed Virtual Switch operations menu. To view the menu options see page 462.
`dpg` Displays the VMware distributed port group operations menu. To view the menu options see page 463.
`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 344. VMware Operations (/oper/virt/vmware) (continued)

Command Syntax and Usage
`dvswitch` Displays the VMware Distributed Virtual Switch operations menu. To view the menu options see page 462.
`dpg` Displays the VMware distributed port group operations menu. To view the menu options see page 463.
`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.

Table 344. VMware Operations (/oper/virt/vmware) (continued)

Command Syntax and Usage
`dvswitch` Displays the VMware Distributed Virtual Switch operations menu. To view the menu options see page 462.
`dpg` Displays the VMware distributed port group operations menu. To view the menu options see page 463.
`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
VMware Distributed Virtual Switch 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
     addUplink - Add a physical NIC to dvSwitch uplink ports
     remUplink - Remove a physical NIC from dvSwitch uplink ports
```

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

Table 345. VMware dvSwitch Operations (/oper/virt/vmware/dvswitch)

Command Syntax and Usage
`add` *<datacenter name> <dvSwitch name> <dvSwitch version>* Adds the specified dvSwitch to the specified DataCenter.
`del` *<datacenter name> <dvSwitch name>* Removes the specified dvSwitch from the specified DataCenter.
`addhost` *<dvSwitch name> <host UUID | IP address | host name>* Adds the specified host to the specified dvSwitch. Use one of the following identifiers to specify the host: – UUID – IP address – Host name
`remhost` *<dvSwitch name> <host UUID | IP address | host name>* Removes the specified host from the specified dvSwitch. Use one of the following identifiers to specify the host: – UUID – IP address – Host name
`addUplink` *<dvSwitch name> <host ID> <uplink name>* Adds the specified physical NIC to the specified dvSwitch uplink ports.
`remUplink` *<dvSwitch name> <host ID> <uplink name>* Removes the specified physical NIC from the specified dvSwitch uplink ports.

/oper/virt/vmware/dpg

VMware 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
```

Use these commands to administer a VMware distributed port group.

Table 346. VMware Distributed Port Group Operations (/oper/virt/vmware/dpg)

Command Syntax and Usage
`add` Adds the specified port group to the specified dvSwitch. You are prompted to enter the following: – Port group name – dvSwitch name – VLAN ID – Ingress shaping (y or n). If “y”, specify the following parameters: • average bandwidth in KB per second (1-1000000000) • burst size in KB (1-1000000000) • peak bandwidth in KB per second (1-1000000000) – Egress shaping (y or n). If “y”, specify the following parameters: • average bandwidth in KB per second (1-1000000000) • burst size in KB (1-1000000000) • peak bandwidth in KB per second (1-1000000000)
`addmac` *<vNIC MAC> <port group name>* Adds the specified VM NIC to the specified port group.

Table 346. VMware Distributed Port Group Operations (/oper/virt/vmware/dpg) (continued)

Command Syntax and Usage
`update` Updates the specified port group on the specified dvSwitch. You are prompted to enter the following: – Port group name – dvSwitch name – VLAN ID – Ingress shaping (e or d) for “enabled or “disabled.” If “e”, specify the following parameters: • average bandwidth in KB per second (1-1000000000) • burst size in KB (1-1000000000) • peak bandwidth in KB per second (1-1000000000) – Egress shaping (e or d) for “enabled or “disabled.” If “e”, specify the following parameters: • average bandwidth in KB per second (1-1000000000) • burst size in KB (1-1000000000) • peak bandwidth in KB per second (1-1000000000)
`del` *<port group name> <dvSwitch name>* Removes the specified port group from the specified dvSwitch.

Chapter 8. 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

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 526.

/boot
Boot Menu

```
[Boot Options Menu]
     stack    - Stacking 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
     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/stack
Stacking Boot Menu

```
[Boot Stacking Menu]
     mode     - Set the stacking mode for the switch
     stktrnk  - Set external 10G ports for Stack Trunks
     vlan     - Set VLAN number for control communication
     clear    - Set stacking parameters to factory default
     ena      - Enable the stacking mode
     dis      - Disable the stacking mode
     cur      - Display current stacking boot parameters
```

The Stacking Boot menu is used to define the role of the switch in a stack: either as the Master that controls the stack, or as a participating Member switch. Options are available for loading stack software to individual Member switches, and to configure the VLAN that is reserved for inter-switch stacking communications.

You must enable Stacking and reset the switch to enter Stacking mode. When the switch enters Stacking mode, the Stacking configuration menu appears. For more information, see "Stacking Configuration Menu" on page 253.

Table 347 lists the Boot Stacking command options.

Table 347. Boot Stacking Options (/boot/stack)

Command Syntax and Usage
`mode master|member` Configures the Stacking mode for the selected switch.
`stktrnk` *<list of ports>* Configures the ports used to connect the switch to the stack. Enter only 10Gb external ports(EXT1, EXT2, EXT3).
`vlan` *<VLAN number>* Configures the VLAN used for Stacking control communication.
`clear` Resets the Stacking boot parameters to their default values.
`ena` Enables the switch stack.
`dis` Disables the switch stack.
`cur` Displays current Stacking boot parameters.

When in stacking mode, the following standalone features are not supported:

- Active Multi-Path Protocol (AMP)
- SFD
- sFlow port monitoring
- Uni-Directional Link Detection (UDLD)
- Port flood blocking
- BCM rate control
- Link Layer Detection Protocol (LLDP)
- Private VLANs
- RIP
- OSPF and OSPFv3
- IPv6
- Virtual Router Redundancy Protocol (VRRP)
- Loopback Interfaces
- Router IDs
- Route maps
- Border Gateway Protocol (BGP)
- MAC address notification
- Static MAC address adding
- Static multicast
- Static routes
- MSTP and RSTP settings for CIST, Name, Rev, and Maxhop
- IGMP Relay and IGMPv3
- Virtual NICs

Switch menus and commands for unsupported features may be unavailable, or may have no effect on switch operation.

/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 348. 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 349. 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.

Updating the Switch Software Image

The switch software image is the executable code running on the 1/10Gb Uplink ESM (GbESM). 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-304.ibm.com/jct01004c/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 or TFTP 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.

Note: When you use a full command on one line in the CLI to perform an FTP/TFTP file transfer, you cannot use a forward slash (/) in the directory path unless it is preceded by a back slash (\ ).

For example, the following is **invalid**:

```
# /boot/gtimg 1 10.10.10.2 image_directory/filename
```

The following is correct:

```
# /boot/gtimg 1 10.10.10.2 image_directory\/filename
```

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

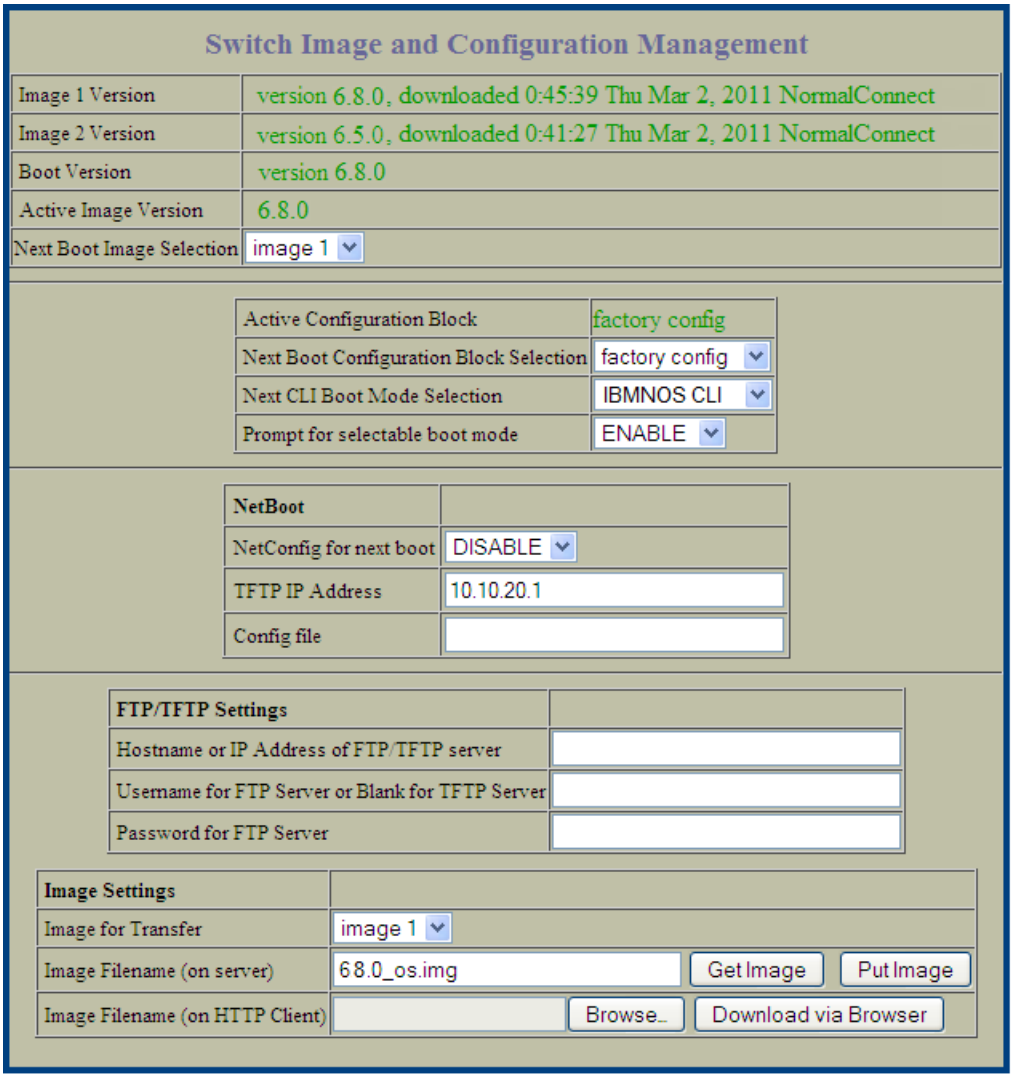
You can use the Browser-Based Interface to load software onto the GbESM. The software image to load can reside in one of the following locations:

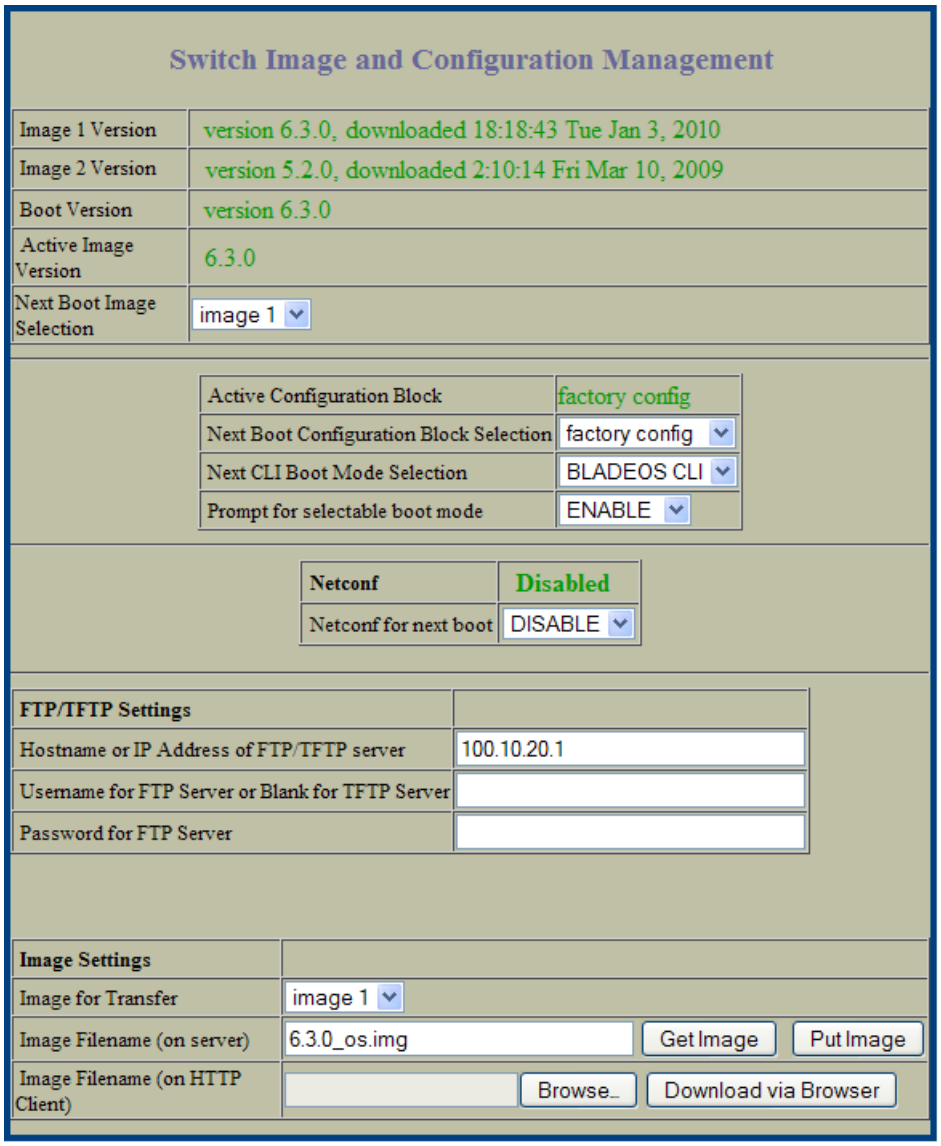
- FTP server
- TFTP server
- Local computer

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 server, enter the server's information in the FTP/TFTP 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 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 server on your network
- The hostname or IPv4/IPv6 address of the FTP/TFTP server
- The name of the new software image or boot file

Note: The DNS parameters must be configured if specifying hostnames. See "Domain Name System Configuration Menu" on page 390.

When the preceding 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 or TFTP server.

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

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

```
Enter name of file on FTP/TFTP server: <filename>
```

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

5. Enter your username for the server, if applicable.

```
Enter username for FTP server or hit return for TFTP server: <username> or <Enter>
```

6. 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 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 IPv4/IPv6 address of the FTP or TFTP server:

```
Enter hostname or IP address of FTP/TFTP server: <name or IP address>
```

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

```
Enter name of file on FTP/TFTP server: <filename>
```

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

```
image2 currently contains Software Version 7.4
 that was downloaded at 0:23:39 Thu Jan  4, 2010.
Upload will transfer image2 (2788535 bytes) to file "image1"
 on FTP/TFTP server 192.1.1.1.
Confirm upload operation (y/n) ? y
```

Selecting a Configuration Block

When you make configuration changes to the GbESM, 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 GbESM 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 GbESM 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 468.

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 GbESM is the IBM N/OS CLI. To access the ISCLI, enter the following command and reset the GbESM:

```
Main# boot/mode iscli
```

To access the IBM N/OS CLI, enter the following command from the ISCLI and reload the GbESM:

```
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 ..............................

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

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

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

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

Recovering from a Failed Upgrade

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

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

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

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

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

```
yzModem - CRC mode, 62494(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** VMLINUX ****

Un-Protected 10 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 10 sectors

**** RAMDISK ****

Un-Protected 44 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 44 sectors

**** BOOT CODE ****

Un-Protected 8 sectors

Erasing Flash..... done

Writing to Flash.....done

Protected 8 sectors
```

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

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

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

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

10. Press <Enter> to continue the download.

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

```
yzModem - CRC mode, 27186(SOH)/0(STX)/0(CAN) packets, 6 retries

Extracting images ... Do *NOT* power cycle the switch.

**** Switch OS ****


Please choose the Switch OS Image to upgrade [1|2|n] :
```

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

```
Switch OS Image 1 ...

Un-Protected 27 sectors

Erasing Flash.............................. done

Writing to Flash.............................done

Protected 27 sectors
```

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

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

14. Press the Escape key (<Esc>) to re-display the Boot Management menu.

    Select 4 to exit and boot the new image.

Chapter 9. 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
     nbrcache - IP6 NBR Cache Manipulation Menu
     route6   - IP6 Route Manipulation Menu
     uudmp    - Uuencode FLASH dump
     ptdmp    - Upload FLASH dump via FTP/TFTP
     ptlog    - Upload file via TFTP
     cldmp    - Clear FLASH dump
     tsdmp    - Tech support dump
     pttsdmp  - Upload tech support dump via FTP/TFTP
```

Dump information contains internal switch state data that is written to flash memory on the 1/10Gb Uplink ESM (GbESM) 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 350. Maintenance Menu (/maint)

Command Syntax and Usage
`sys` Displays the System Maintenance Menu. To view menu options, see page 483.
`fdb` Displays the Forwarding Database Manipulation Menu. To view menu options, see page 484.
`debug` Displays the Debugging Menu. To view menu options, see page 485.
`dcbx` Displays the DCBX Debugging Menu. To view menu options, see page 486
`lldp` Displays the LLDP Cache Manipulation Menu. To view menu options, see page 487.

Table 350. Maintenance Menu (/maint)

Command Syntax and Usage
`arp` Displays the ARP Cache Manipulation Menu. To view menu options, see page 488.
`route` Displays the IP Route Manipulation Menu. To view menu options, see page 489.
`igmp` Displays the IGMP Maintenance Menu. To view menu options, see page 490.
`mld` Displays the MLD Multicast Group Maintenance Menu. To view menu options, see page 493.
`nbrcache` Displays the IPv6 Neighbor Cache Manipulation Menu. To view menu options, see page 494.
`route6` Displays the IPv6 Route Manipulation Menu. To view menu options, see page 494.
`uudmp` Displays dump information in uuencoded format. For details, see page 495.
`ptdmp` *<host name> <file name>* Saves the system dump information via TFTP. For details, see page 495.
`ptlog` Saves the system log file (SYSLOG) via TFTP.
`cldmp` Clears dump information from flash memory. For details, see page 496.
`tsdmp` Dumps all GbESM information, statistics, and configuration.You can log the tsdump output into a file.
`pttsdmp` Redirects the technical support dump (tsdmp) to an external TFTP 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 351. 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
     mcdump   - Display all Multicast MAC entries added
     mcreload - Reload all Multicast MAC entries
```

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 352. 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 51.
`del` *<MA1C address>* [*<VLAN number>*] Removes a single FDB entry.
`clear` Clears the entire Forwarding Database from switch memory.
`mcdump` Displays all Multicast MAC entries in the FDB.
`mcreload` Reloads static Multicast MAC entries.

/maint/debug

Debugging Menu

```
[Miscellaneous Debug Menu]
     tbuf     - Show MP trace buffer
     snap     - Show MP snap (or post-mortem) trace buffer
     clrcfg   - Clear all flash configs
```

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

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 353. 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.

`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.

/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 354. 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
     instance - Show LLDP remote devices information
     dump     - Show all LLDP information
     clear    - Clear LLDP remote devices information
```

Table 355 describes the LLDP cache manipulation commands.

Table 355. 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.
`instance` Displays instance information received from LLDP -capable devices.
`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 356 describes the ARP cache maintenance menu options.

Table 356. 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 74.

/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
```

Table 357 describes the IPv4 route manipulation menu options.

Table 357. 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 34 on page 72.
`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 35 on page 73.
`if` *<interface number>* Shows routes on a single interface.
`dump` Shows all routes.
`clear` Clears the route table from switch memory.

Note: To display all routes, you can also refer to “IPv4 Routing Information” on page 71.

/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 358 describes the IGMP Maintenance commands.

Table 358. IGMP Maintenance Menu Options (/maint/igmp)

Command Syntax and Usage
`group` Displays the Multicast Group menu. To view menu options, see page 491.
`mrouter` Displays the Multicast Router Port menu. To view menu options, see page 490.
`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 359 describes the IGMP Maintenance commands.

Table 359. 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.
`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 360 describes the IGMP multicast router (Mrouter) maintenance commands.

Table 360. 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 362 describes the IPv6 Neighbor Discovery cache manipulation options.

Table 361. IPv6 Neighbor Discovery Cache Manipulation (/maint/nbrcache)

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/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 362 describes the IPv6 Neighbor Discovery cache manipulation options.

Table 362. 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 363 describes the IPv6 Route maintenance options.

Table 363. 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 496.

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 server> <filename>*
FTP/TFTP System Dump Put

Use this command to `put` (save) the system dump to a FTP/TFTP server.

Note: If the FTP/TFTP 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, at the `Maintenance#` prompt, enter:

```
Maintenance# ptdmp <FTP/TFTP server> <filename>
```

Where *server* is the FTP/TFTP server IPv4/IPv6 address or hostname, and *filename* is the target dump file.

/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, 2010. 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. IBM N/OS System Log Messages

The 1/10Gb Uplink ESM (GbESM) uses the following syntax when outputting system log (syslog) messages:

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

The following parameters are used:

- <*Timestamp*>

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

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

  For example: Aug 19 14:20:30

- <*Log Label*>

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

- <*Thread ID*>

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

- <*Message*>: The log message

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

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

LOG_ALERT

Thread	LOG_ALERT Message
	Possible buffer overrun attack detected!
AMP	AMP group <group> topology is DOWN
AMP	AMP keep-alive timeout on {port *<port>* | trunk *<trunk ID>*}
AMP	AMP packets looped back on {port *<port>* | trunk *<trunk ID>*}
AMP	Discarding BPDUs received on port *<port>* while AMP is enabled
AMP	Dropping AMP v*<group>* packets received on {port *<port>* | trunk *<trunk ID>*}, expecting v*<AMP version>*
AMP	Port *<port>* is disabled by AMP BPDU guard
AMP	Putting port *<port>* in blocking state
BGP	Invalid notification (Code:*<code>*, Subcode:*<subcode>*) received from *<IP address>*
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

Thread	LOG_ALERT Message (continued)
BGP	session with <*IP address*> failed (<*reason type*>) : (<*reason*>) Reason Types: • Cease • FSM Error • Hold Timer Expired • Message Header Error • Null Error Code • OPEN Message Error • UPDATE Message Error Reasons: • AS Routing Loop • Attr Flags Error • Attr Length Error • Auth Failure • Bad BGP Identifier • Bad HoldTime • Bad Length • Bad Peer AS • Bad Type • Conn Not Synced • Invalid Network Field • Invalid NEXTHOP Attr • Invalid ORIGIN Attr • Malformed AS_PATH • Malformed Attr List • Missing Well Known Attr • None • Optional Attr Error • Unrecognized Well Known Attr • Unsupported Opt Param • Unsupported Version
HOTLINKS	LACP trunk <*trunk ID*> and <*trunk ID*> formed with admin key <*key*>
IP	cannot contact default gateway <*IP address*>
IP	Dynamic Routing table is full
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
RMON	Event.<*description*>
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

Thread	LOG_ALERT Message (continued)
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.
STP	STG *<STG>* preferred Fast Uplink port *<port>* active. Waiting *<seconds>* seconds before switching from port *<port>*
STP	STG *<STG>* root port *<port>* has gone down. Putting backup Fast Uplink port *<port>* into forwarding
STP	STG *<STG>*, new root bridge
STP	STG *<STG>*, topology change detected
SYSTEM	*<SFP type>* incorrect device in port *<port>*. Device is DISABLED.
SYSTEM	*<SFP type>* inserted at port *<port>* is UNAPPROVED !
SYSTEM	*<SFP type>* inserted at port *<port>* is UNAPPROVED ! {DAC|SFP|SFP+|XFP|???} is DISABLED.
SYSTEM	Ingress PVST+ BPDU's spotted from port *<port>*
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	<*port*> WRONG Type (SFP vs SFP+)
SYSTEM	<*SFP type*> inserted at port <*port*> has I2C FAILURE ! {DAC|SFP|SFP+|XFP|???} is DISABLED.
SYSTEM	Failed to Read <*SFP type*> {ID|Temperature|Voltage} for port {<*port*>|???}
SYSTEM	Failed to Write Select I2C MUX for sfp <*port*>
SYSTEM	Poll SFP/XFP Failed to get Status
SYSTEM	System memory is at <*n*> percent
SYSTEM	Temp back to normal
SYSTEM	TEMP CAUTION DETECTED
SYSTEM	Temperature (<*temperature*>) is OVER Range on port <*port*>
SYSTEM	TX Fault on port <*port*>. {DAC|SFP|SFP+|XFP|???} is DISABLED.
SYSTEM	Voltage (<*voltage*>) is OVER Range on port <*port*>

LOG_ERR

Thread	LOG_ERR Message
CFG	Can't assign a port with same protocol to different VLANs.
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	ERROR: Cannot enable/disable RMON for Mgmt Port <*port*>
CFG	ERROR: More than <maximum> VLAN(s) in downstream
CFG	Have not defined protocol type!
CFG	Management VLAN cannot be a private-VLAN.
CFG	Management VLAN cannot support protocols.
CFG	Maximum allowed number (30) of Alarm groups have already been created.
CFG	Maximum allowed number (30) of Event groups have already been created.
CFG	Maximum allowed number (5) of History groups have already been created.
CFG	Need to enable port's tag for tagging pvlan.
CFG	Overflow! Port has more than 16 protocols.
CFG	Port is not for this protocol.
CFG	Switch rem port fails when disable {protocol|vlan}.
CFG	TFTP {Copy|cfgRcv} attempting to redirect a previously redirected output
ETS	The internal COS7 is used for stack communication; hence the ETS priority group 7 is not available.
IP6	EXCEPTIONAL CASE Trying to create IP6 Interface after the Ip6Shutdown
IP6	Ip6IfRcvPkt(alloc,failed):if=<*interface*>
IP6	Ip6Lanif(down,failed):if=<*interface*>,rc=<*reason code*>
IP6	Ip6Lanif(llStatus=<*status*>,failed):if=<*interface*>,rc=<*reason code*>
IP6	Ip6SetAddr(failed):if=<*interface*>, addr <*IPv6 address*>, rc=<*reason code*>

Thread	LOG_ERR Message (continued)
IP6	IPv6 route table full
IP6	ipv6_add_interface_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_nbrcache_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_add_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_prefix_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_rem_route_immediate: Buffer Non Linear for ip6_cfa_params
IP6	ipv6_vlan_change_immediate: Buffer Non Linear for ip6_cfa_params
LLDP	Port <*port*>: Cannot add new entry. MSAP database is full!
MGMT	Apply is issued by another user. Try later[.]
MGMT	Attempting to add the Mgt Default Route with the Mgt IP Interface (<*interface*>) DISABLED.
MGMT	Critical Error. Failed to {add|attach} Loopback Interface <*interface*>
MGMT	Critical Error failed to add Interface <*interface*>
MGMT	Critical Error.Failed to add Interface <*interface*>
MGMT	Critical Error.Failed to detach Loopback Interface <*interface*> rc=<*reason code*>
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: Apply not done. Use "diff" to see pending changes, then use configuration menus to correct errors.
MGMT	ERROR: Cannot enable {OSPF|OSPFv3} on Management interface.
MGMT	Error: Invalid {image1|image2}
MGMT	Error: Pushed {image1|image2} size <*bytes*> bigger than the capacity <*maximum bytes*>.
MGMT	Error: Save not done.
MGMT	Firmware download failed (insufficient memory
MGMT	Invalid CRC value. Boot image rejected
MGMT	Revert Apply is issued by another user. Try later.
MGMT	Revert is issued by another user. Try later.

Thread	LOG_ERR Message (continued)
MGMT	Save is issued by another user. Try later.
MGMT	unapplied changes reverted
MGMT	VPD_IP_STATIC - add_address *<IP address>* failed
MGT	You are attempting to load an image that has been corrupted or belongs to another switch type. Please verify you have the correct file for this switch and try again. [Error: Invalid header magic value <value>.] Boot image rejected
NTP	unable to listen to NTP port
PFC	PFC can be enabled on 2 priorities only - priority 3 and one other priority.
RMON	Maximum {Alarm|Event|History} groups exceeded when trying to add group *<group>* via SNMP
STACK	Boot Image could not be successfully received by *<MAC adress>*.Resending it.
STACK	Config File could not be successfully received by *<MAC adress>*.Resending it.
STACK	File *<File ID>* could not be successfully received by *<MAC adress>*.Resending it.
STACK	Image{1|2} could not be successfully received by *<MAC adress>*.Resending it.
STACK	Incorrect xfer status: from *<MAC adress>* for {Boot Image|Image1|Image2|Config File|File *<File ID>*} status *<status>*
STACK	Switch with duplicate MAC (*<MAC address>*) trying to join.
STACK	The joining of switch (*<MAC address>*) in BCS chassis bay *<bay number>* with different port mapping is denied
STACK	The joining of switch (*<MAC address>*) with different chassis type *<chassis type>* is denied
STACK	The joining of switch (*<MAC address>*) with different type *<switch type>* is denied
STACK	The master is in BCS chassis bay *<bay number>* with different port mapping
STP	Cannot set "{Hello Time|Max Age|Forward Delay|Aging}" (Switch is in MSTP mode)
SYSTEM	Error: BOOTP Offer was found incompatible with the other IP interfaces
SYSTEM	Error: DHCP Offer was found invalid by ip configuration checking;[ ]please see system log for details.
SYSTEM	I2C device *<ID>* *<description>* set to access state *<state>* [from CLI]

Thread	LOG_ERR Message (continued)
SYSTEM	Not enough memory!
SYSTEM	{PortChannel | Trunk group} creation failed for {IntPortChannel | PortChannel | Internal Trunk group | Trunk group} <*trunk ID*>. Only <*maximum trunks*> {PortChannels | Trunk groups} supported by hardware.
TFTP	Error: Receive file from the master failed for <*file ID*>.
TFTP	Error: Receive transfer of config file from the master failed
TFTP	Error: Receive transfer of image1 | 2 from the master failed
TFTP	Error: Sending of {boot image | config file | image1 | image2} to switch <*MAC address*> failed
TFTP	TFTP Copy attempting to redirect a previously redirected output

LOG_INFO

Thread	LOG_INFO Message
	System log cleared by user *<username>*.
	System log cleared via SNMP.
DIFFTRAK	/* Config changes at <time> by *<username>* */ *<config diff>* /* Done */
HOTLINKS	"Error" is set to "{Active|Standby}"
HOTLINKS	has no "{Side Max|None|Learning|Error}" interface
HOTLINKS	"Learning" is set to "{Active|Standby}"
HOTLINKS	"None" is set to "{Active|Standby}"
HOTLINKS	"Side Max" is set to "{Active|Standby}"
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	All local control functions are enabled when PRM mode is activated
MGMT	boot config block changed
MGMT	Boot image ({Boot|Kernel|FS}, *<size>* bytes) download complete.
MGMT	boot image changed
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	boot kernel downloaded from the master, softer version *<version>*
MGMT	Boot Sector now contains Software Version *<version>*
MGMT	Can't downgrade to image with only single flash support
MGMT	/* Config changes at <time> by *<username>* */ *<config diff>* /* Done */
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	Failover just occurred, please try later

Thread	LOG_INFO Message (continued)
MGMT	Firmware download failed to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}
MGMT	Firmware downloaded to {invalid image | image1 | image2 | boot kernel | undefined | SP boot kernel}.
MGMT	Flash dump successfully tftp'd to *<hostname>*:*<filename>*
MGMT	FLASH ERROR - invalid address used
MGMT	Flash Read Error. Failed to read flash into holding structure. Quitting
MGMT	Flash Write Error
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	Forced unit detach detected, please try later
MGMT	FS Sector now contains Software Version *<version>*
MGMT	image{1 | 2} download completed. Now writing to flash.
MGMT	image{1 | 2} downloaded {from host *<hostname>* | via browser}, filename too long to be displayed, software version *<version>*
MGMT	image{1 | 2} downloaded from host *<hostname>*, file'*<filename>*', software version *<version>*
MGMT	image{1 | 2} downloaded from the master, softer version *<version>*
MGMT	image{1 | 2} now contains 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	invalid image downloaded from the master, softer version *<version>*
MGMT	iSP boot kernel downloaded from the master, softer version *<version>*
MGMT	Kernel Sector now contains Software Version *<version>*
MGMT	NETBOOT: Config successfully downloaded and applied from *<hostname>*:*<filename>*
MGMT	New config set

Thread	LOG_INFO Message (continued)
MGMT	new configuration applied [from {BBI|EM|NETBOOT|SCP|SNMP|Stacking Master}]
MGMT	new configuration saved [from {BBI|BladeOS|ISCLI|SNMP}]
MGMT	Please save your current configuration and restart the stack.
MGMT	Protected Mode is already OFF.
MGMT	Revert failed: configuration is dumped or modified by another user.
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	Sector now contains Software Version <*version*>
MGMT	Setting of Mgmt VLAN Interface cannot be changed to Disabled
MGMT	SP boot kernel download completed. Now writing to flash.
MGMT	SP boot kernel downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	SP boot kernel downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	Starting Firmware download for {invalid image|image1|image2|boot kernel|undefined|SP boot kernel}[.]
MGMT	Static FDB entry on disabled VLAN
MGMT	Tech support dump failed
MGMT	Tech support dump successfully tftp'd to <*hostname*>:<*filename*>
MGMT	Two Phase Apply Failed in Creating Backup Config Block.
MGMT	undefined download completed. Now writing to flash.
MGMT	undefined downloaded {from host <*hostname*>|via browser}, filename too long to be displayed, software version <*version*>
MGMT	undefined downloaded from host <*hostname*>, file '<*filename*>', software version <*version*>
MGMT	undefined downloaded from the master, softer version <*version*>
MGMT	unsaved changes reverted [from {BBI|SNMP}]
MGMT	unsaved changes reverted except the backup [from BBI|from SNMP]
MGMT	Unsupported GBIC {accepted|refused}
MGMT	user {SNMP user|<*username*>} ejected from BBI

Thread	LOG_INFO Message (continued)
MGMT	Verification of new {invalid image|image1|image2|boot kernel|undefined|SP boot kernel} in FLASH successful.
MGMT	WARNING WARNING WARNING WARNING!!!!!!!!!! CRC Error detected in BOOT region ({Boot|Kernel|FS}) - download another image and DO NOT reset your switch
MGMT	WARNING: A Reboot is required for the new downloaded image to take effect.
MGMT	Watchdog has been {enabled|disabled}
MGMT	Watchdog timeout interval is now *<seconds>* seconds)
MGMT	Writing to flash...This can take up to {90|150} seconds. Please wait
MGMT	Wrong config file type
MGMT	You must enable permission for control of {External Management|External Ports|Factory Default Reset|Mgmt VLAN Interface} from the MM [or you must Disable this feature.]
MGMT	You must select at least one PRM Feature to turn on
RMON	RMON {alarm|event|history} index *<ID>* was deleted via SNMP
RMON	SNMP configuration for RMON {alarm|event|history} index *<ID>* applied
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 {image1|image2}, {active|backup|factory} config block
SYSTEM	FDB Learning {DISABLED|ENABLED} for port *<port>*
TFTP	Successfully sent {boot image|image1|mage2} to switch *<MAC adress>*

LOG_NOTICE

Thread	LOG_NOTICE Message
	<*minutes*> minute(s) until scheduled reboot
	ARP table is full.
	Could not create check point entry for {DCBX|VNIC}
	Current config successfully tftp'd to <*hostname*>: <*filename*>
	ECMP route configured, Gateway health check enabled
	Evaluation period has expired. To purchase a Full license for this software, please visit www.bladenetwork.net/services or email: services@bladenetwork.net
	External port <*port*> disabled
	More than one trunk found for LACP adminkey <*adminkey*>. Static MAC entry <*index*> was added only to trunk <*trunk number*>.
	Port <*port*> mode is changed to full duplex for 1000 Mbps operation.
	Tech support dump successfully tftp'd to <*hostname*>: <*filename*>
	scheduled switch reboot
	switch reset at <*time*> has been canceled
	switch reset scheduled at <*time*>
8021X	Authentication session terminated with {Failure|Success} on port <port>
8021X	Could not create failover checkpoint record for port <port>
8021X	Logoff request on port <port>
8021X	Port <port> {assigned to|removed from} vlan <VLAN>
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Medium-Type value (<tunnel type>); should be 6 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> has an invalid Tunnel-Type value (<tunnel type>); should be 13 for VLAN assignment
8021X	RADIUS server <IP address> auth response for port <port> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a non-existent or disabled VLAN, and cannot be assigned to port <port>
8021X	RADIUS server <IP address> auth response has a VLAN id (<VLAN>) of a reserved VLAN and cannot be assigned to port <port>

Thread	LOG_NOTICE Message (continued)
8021X	RADIUS server <IP address> auth response has an invalid VLAN id (<VLAN>) and cannot be assigned to port <port>
BGP	authentication receive error from <IP address>
BGP	bad authentication received from <IP address>
BGP	no authentication received from <IP address>
BGP	session established with <IP address>
DCBX	Detected DCBX peer on port <port>
DCBX	LLDP {RX|TX} is disabled on port <port>
DCBX	LLDP TX & RX are 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	<MAC address> has been reassigned, the old connection will be deleted.
FCOE	Failed to create FCOE vlan <VLAN>
FCOE	FCF <MAC address> has been removed.
FCOE	FCF <MAC address> is now operational.
FCOE	FCOE vlan <VLAN> created.
FCOE	Port <port> has been added to the FCOE vlan <VLAN>.
IP	cannot contact multicast router <IP address>
IP	default gateway <IP address> {disabled|enabled|operational}
IP	Either ECMP, Route or Arp table is full.Please check GEA L3 and ECMP statistics (/stat/l3/gea) to verify.
IP	L3 table is full. Please check GEA L3 statistics (/stat/l3/gea) to verify.
IP	mrouter <IP address> has been disabled or deleted
IP	multicast router <IP address> operational
IP	Received {IGMPv1|IGMPv2} query from <IP address>
IP	VLAN <VLAN> is not in the igmp relay list. Mrouter <IP address> will be down
IP	Warning: Enabling dhcp will delete IP interface <interface> and IP gateway <gateway>'s configurations.
IP	Warning: Enabling dhcp will delete master switch IP interface and default gateway configurations.
LACP	LACP is {up|down} on port <port>

Thread	LOG_NOTICE Message (continued)
LINK	link up on port <port>
MGMT	<username> automatically logged out from BBI because changing of authentication type
MGMT	<username>(<user type>) {logout|idle timeout} from BBI
MGMT	Authentication failed for backdoor.
MGMT	Authentication failed for backdoor. Telnet disabled!
MGMT	boot config block changed
MGMT	boot image changed
MGMT	boot mode changed
MGMT	Chassis Control of External Ports can not be changed thru I2C Control Register
MGMT	Chassis Control of Management via all ports can not be changed thru I2C Control Register
MGMT	Chassis Control of Reset Factory Defaults can not be changed thru I2C Control Register
MGMT	DAD found duplicate IP address on management interface <interface>
MGMT	enable password changed
MGMT	External Ports {DISABLED|ENABLED} thru I2C Control Register
MGMT	External Ports can not be DISABLED thru I2C Control Register
MGMT	Failed login attempt via BBI from host <IP address>.
MGMT	Failed login attempt via the CONSOLE
MGMT	FLASH Dump cleared from BBI
MGMT	Invalid Chassis SubType (<subtype>) detected, assuming {BCT|BC}
MGMT	Invalid IOBay (<IOBay ID>) detected, assuming ex@top-ex in@bot.
MGMT	Invalid SlotID (<slot ID>) detected, assuming Slot 1.
MGMT	Local Control of External Ports ENABLED thru Protected Mode
MGMT	Local Control of Management via all ports ENABLED thru Protected Mode
MGMT	Local Control of Mgmt VLAN Interface from VPD ENABLED thru Protected Mode
MGMT	Local Control of Reset Factory Defaults is ENABLED thru Protected Mode
MGMT	Management Port {1|2} RESET thru I2C Control Register

Thread	LOG_NOTICE Message (continued)
MGMT	Management STG 16 configurations from old config file moved to STG 32
MGMT	Management via all ports cannot be DISABLED thru I2C Control Register
MGMT	Management via all ports ENABLED thru I2C Control Register
MGMT	Membership for Port <port> in vlan <VLAN> is not effective while the port is assigned with PVID <PVID> by 802.1x
MGMT	Method {STATIC|DHCP|DISABLED}, IP Address *<IP address>*, Mask *<netmask>*[, Gateway *<IP address>*]
MGMT	Method {STATIC|DHCPv6|DISABLED|STATELESS} IP Address *<IPv6 address>*/*<prefix length>*[, Gateway *<IPv6 address>*]
MGMT	Mgt Gateway <IP address> has the same IP addres as the Mgt IP
MGMT	New Management Gateway <IP address> configured [default]
MGMT	New Management IP Address <IP address> configured
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	Port <port> remains untagged while it is assigned PVID <PVID> by 802.1x
MGMT	Port <port> was not enabled because it is disabled thru configuration.
MGMT	Protected Mode Mismatch : MM capabilities is not a subset of MMpermissions.
MGMT	Protected Mode Mismatch : MM Config inconsistent with SM Config.
MGMT	Protected Mode Mismatch : SM retains PRM local control of previously selected features.
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	secondSYSLOG host changed to {this host|<IP address>}
MGMT	selectable [boot] mode changed

Thread	LOG_NOTICE Message (continued)
MGMT	STM Warning : Chassis does NOT support stacking mode.
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	Terminating BBI connection from host <IP address>
MGMT	Updated switch image to match master's image version. Reset needed
MGMT	User <username> deleted by {SNMP user|<username>}.
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}
OSPFV3	Link state database is FULL.Ignoring LSA.
OSPFV3	nbr <router ID> changes state from {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL} to {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL}[, Neighbor Down: {Interface down or detached|Dead timer expired}]
OSPFV3	virtual link nbr <router ID> changes state from {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL} to {DOWN|ATTEMPT|INIT|2WAY|EXSTART|EXCHANGE|LOADING|FULL}[, Neighbor Down: {Interface down or detached|Dead timer expired}]
SERVER	[link|Link] {down|up} on port <port>
STACK	<MAC address> become master {after init|from backup}
STACK	a specified master switch just joined the stack
STACK	A switch (<MAC address>) with no csnum assigned just joined.
STACK	attached switch <MAC address> cleared
STACK	BACKUP_GONE|BACKUP_PRESENT received from the master <MAC address>
STACK	BE_BACKUP|BE_MEMBER received from the master <MAC address>
STACK	BE_BACKUP|BE_MEMBER sent to <MAC address>
STACK	Boot Image successfully received by <MAC address>
STACK	CFG_REQ {received from|sent to} <MAC address>
STACK	CFG_SCRIPT received from the master <MAC address>
STACK	CFG_SCRIPT sent to <MAC address>

Thread	LOG_NOTICE Message (continued)
STACK	Config File successfully received by <MAC address>>
STACK	Current switch state changed, {all current sessions|current console session} will be terminated.
STACK	DCS from non-master received
STACK	DELAYED_REBOOT timer expired
STACK	File <File ID> successfully received by <MAC address>
STACK	FORCED_DETACH received from the master <MAC address>
STACK	FORCED_DETACH sent to <MAC address>
STACK	I_AM_BACKUP sent to <MAC address>
STACK	I_AM_MASTER received from the master <MAC address>
STACK	Image1|2 successfully received by <MAC address>
STACK	ingress application traffic {are blocked|is resumed}
STACK	JOIN_STACK received from <MAC address>
STACK	LEAVE_STACK received from <MAC address>
STACK	Link down on stack port <csnum>:<port> (MAC <MAC address>)
STACK	Link down on stack port <port>:(MAC <MAC address>)
STACK	Link up on stack port <csnum>:<port>
STACK	local csnum changed to <csnum>
STACK	local ports disabled by {local master|local switch|the master}
STACK	local ports enabled by {local master|the master}
STACK	Member could not send the status of the tftp transfer to the master
STACK	Member switch booted with <A> cosQ.Master switch has <B> cosQ. Resetting to update.
STACK	merger of two stacks detected [on remote switch <MAC address>
STACK	more than one specified master switches joined the stack
STACK	Newly {attached|configured} switch's boot config is {active|backup|factory}, updating to {active|backup|factory}
STACK	Newly attached switch's cosQ configuration is <A> Not matching Master's cosQ configuration <B>, updating.
STACK	Newly attached switch's flash version is <version>.Not matching Master's version, updating image <image>
STACK	Newly attached switch's NetConfig is {enabled|disabled}, updating to{enabled|disabled}

Thread	LOG_NOTICE Message (continued)
STACK	Newly attached switch's version matches Master's flash, but not current version. Please reset Master to allow new members to join.
STACK	Newly attached switch's version matches Master's version. Rebooting attached switch.
STACK	no master present now while one existed before
STACK	Not matching Master's boot image <version>, updating.
STACK	old master disappeared
STACK	PARAM_REQ_ATTACH received from the master <MAC address>
STACK	REQ_ATTACH received from <MAC address>
STACK	requested to reboot by the master
STACK	STACK: <SFP type> inserted at port <csnum>:<port> is {APPROVED|UNAPPROVED}
STACK	STACK: <SFP type> removed at port <csnum>:<port>
STACK	switch {apply|revert|revert apply} from DC
STACK	Switch <csnum>[,] <MAC address> just joined.
STACK	TO_JOIN_STACK {received from|sent to} <MAC address>
STP	Cannot set <parameter> (Switch is in MSTP mode)
SYSTEM	<SFP type> inserted at port <port>
SYSTEM	Address for interface <interface> ignored because of mismatch.
SYSTEM	Change fiber GIG port <port> speed to 1000
SYSTEM	Changed ARP entry for IP <IP address> to: MAC <MAC address>, Port <port>, VLAN <VLAN>
SYSTEM	Could NOT read Active Cable Compliance
SYSTEM	ECMP route gateway <IP address> [via if <interface>] is {down|up}
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	Failed to read 10Gb Compliance (SR/LR) for <SFP type> <port>.
SYSTEM	Failed to read cable length for DAC.
SYSTEM	Failed to read Connector Type (OPT/CX4) for <SFP type> <port>.
SYSTEM	Ingress PVRST BPDU's spotted from port <port>
SYSTEM	L2 table is full!
SYSTEM	Mask for interface <interface> ignored because of mismatch.
SYSTEM	Port <port> disabled by OAM (unidirectional|TX-RX Loop)
SYSTEM	Port <port> disabled by PVST Protection

Thread	LOG_NOTICE Message (continued)
SYSTEM	Port <port> disabled due to reason code <reason code>
SYSTEM	rebooted <time of last reboot>
SYSTEM	Received BOOTP Offer: IP: <IP address> Mask: <netmask> Broadcast <IP address> GW: <IP address>
SYSTEM	Received DHCP Offer: IP: <IP address> Mask: <netmask> Broadcast <IP address> GW: <IP address>
SYSTEM	Received DHCPv6 Reply for IF <interface> IPv6: <IPv6 address> Prefix: <prefix length>
SYSTEM	server with MAC address <MAC address> was {added to|removed from} network
SYSTEM	SM_PRM_Control change FAILED.
SYSTEM	SM_PRM_Control changed.
SYSTEM	Static route gateway *<IP address>* [via if *<interface>*] is {down|up}
SYSTEM	Watchdog threshold changed from <old value> to <new value> seconds
SYSTEM	Watchdog timer has been {enabled|disabled}
VLAN	Default VLAN can not be deleted
VM	Could not create check point entry for VM MAC [HOST]
VM	Virtual Machine with {IP address *<IP address>*|MAC address *<MAC address>*} changed its VLAN to *<new VLAN>*. It was previously in VLAN *<old VLAN>*
VM	Virtual Machine with {IP address *<IP address>*|MAC address *<MAC address>*} is a member of VLAN *<VLAN>*
VM	Virtual Machine with MAC address *<MAC address>* moved to a non-server port.
VM	VM agent resumed (Refresh).
VM	VM agent resumed (Scan).
VM	VM agent: local table full.
VM	VM MAC *<MAC address>* not added to hash table
VM	VM MAC *<MAC address>* NOT added to hash table
VM	VM move detected but failed to move network conf
VRRP	virtual router *<IP address>* is now {BACKUP|MASTER}
WEB	*<username>* ejected from BBI
WEB	*<username>* ejected from BBI because username/password was changed

LOG_WARNING

Thread	LOG_WARNING Message
	Changing numcos sets up the default COSq configuration. Please see diff.
	There is an IP address (<*IP address*>) conflict on the network.
8021X	Authentication session terminated with {Failure|Success} on port <*port*>
8021X	Could not create failover checkpoint record for port <*port*>
8021X	Logoff request on port <*port*>
8021X	Port <*port*> {assigned to|removed from} vlan <*VLAN*>
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Type value (<*tunnel type*>); should be 13 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> has an invalid Tunnel-Medium-Type value (<*tunnel type*>); should be 6 for VLAN assignment
8021X	RADIUS server <*IP address*> auth response for port <*port*> is missing one or more tunneling attributes for VLAN assignment
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a reserved VLAN and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has a VLAN id (<*VLAN*>) of a non-existent or disabled VLAN, and cannot be assigned to port <*port*>
8021X	RADIUS server <*IP address*> auth response has an invalid VLAN id (<*VLAN*>) and cannot be assigned to port <*port*>
AMP	Access port <*port*> is receiving AMP packets from {access|aggregator} switch <*MAC address*>
AMP	Access trunk <*trunk ID*> is receiving AMP packets from {access|aggregator} switch <*MAC address*>
AMP	Aggregator {port <*port*>|trunk <*trunk ID*>} is receiving AMP packets from access switch <*MAC address*>
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*>.
CFG	Switch cannot support more than 16 protocols simultaneously!
CFG	Unfit config exists when protocol-vlan apply.

Thread	LOG_WARNING Message (continued)
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
IP	*<IP address>* configured as V{1|2} and received IGMP V{2|1} query
MGMT	Management Ports 1 and 2 DISABLED because Management Module 1 and 2 are BOTH IN-ACTIVE
NTP	cannot contact any NTP server
NTP	cannot contact [primary|secondary] NTP server *<IP address>*
STACK	no master present in the stack so far
STACK	The specified backup (*<csnum>*) is the current master - a specified master; no backup will be selected in this case
SYSTEM	*<SFP type>* removed at port *<port>*
SYSTEM	Failed to read status register
SYSTEM	I2C device *<ID>* *<description>* set to access state *<state>* [from CLI]
SYSTEM	Interface <interface> failed to renew DHCP Lease.
SYSTEM	transceiver missing at port *<port>*
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. IBM N/OS SNMP Agent

SNMP Overview

The IBM N/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 26543.

Detailed SNMP MIBs and trap definitions of the IBM N/OS SNMP agent are contained in the following IBM N/OS enterprise MIB document:

GbESM-10Ub-L2L3.mib

The IBM N/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 N/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 N/OS:

Table 364. IBM N/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.

Table 364. IBM N/OS-Supported Enterprise SNMP Traps (continued)

Trap Name	Description
altSwValidLogin	Signifies that a user login has occurred.
altSwValidLogout	Signifies that a user logout has occurred.
altSwNtpNotServer	An altSwNtpNotServer trap is sent when cannot contact primary or secondary NTP server.
altSwNtpUpdateClock	An altSwNtpUpdateClock trap is sent when received NTP update.

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 365.

Table 365 lists the MIBS used to perform operations associated with the Switch Image and Configuration files.

Table 365. MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTransferServer	1.3.6.1.4.1872.2.5.1.1.7.1.0
agTransferImage	1.3.6.1.4.1872.2.5.1.1.7.2.0
agTransferImageFileName	1.3.6.1.4.1872.2.5.1.1.7.3.0
agTransferCfgFileName	1.3.6.1.4.1872.2.5.1.1.7.4.0
agTransferDumpFileName	1.3.6.1.4.1872.2.5.1.1.7.5.0
agTransferAction	1.3.6.1.4.1872.2.5.1.1.7.6.0
agTransferLastActionStatus	1.3.6.1.4.1872.2.5.1.1.7.7.0
agTransferUserName	1.3.6.1.4.1872.2.5.1.1.7.9.0
agTransferPassword	1.3.6.1.4.1.1872.2.5.1.1.7.10.0
agTransferTSDumpFileName	1.3.6.1.4.1.1872.2.5.1.1.7.11.0

The following SNMP actions can be performed using the MIBs listed in Table 365.

- 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. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

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

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

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

Using the documentation

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

Getting help and information on the World Wide Web

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

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

Software service and support

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

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

Hardware service and support

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

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

IBM Taiwan product service

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

IBM Taiwan product service contact information:

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

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W