Command Reference

Alteon OS™ 21.0

Layer 2-3 GbE Switch Module for IBM @server BladeCenter

Part Number: 59P4353, December 2004

NORTEL NETWORKS™

4655 Great America Parkway
Santa Clara, CA 95054
www.nortelnetworks.com
Reference: 217025-A

Contents

Preface

The *Alteon OS 21.0 Command Reference* describes how to configure and use the Alteon OS software with your GbE Switch Module.

For documentation on installing the switches physically, see the *Installation Guide* for your GbE Switch Module.

Who Should Use This Book

This *Command Reference* 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, "Alteon OS Syslog Messages," shows a listing of syslog messages.

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

"Glossary" includes definitions of terminology used throughout the book.

"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	Example
`AaBbCc123`	This type is used for names of commands, files, and directories used within the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`Main#`
`AaBbCc123`	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **`sys`**
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** `[`**`-a`**`]`

How to Get Help

If you need help, service, or technical assistance, see the “Getting help and technical assistance” appendix in the Nortel Networks *Layer 2-3 GbE Switch Module for IBM eServer BladeCenter Installation Guide* on the IBM *BladeCenter Documentation* CD.

CHAPTER 1
The Command Line Interface

Your GbE Switch Module 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 Alteon 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
- Alteon 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 via the management module
- Using a Telnet connection over the network
- Using a SSH connection to securely log into another computer over a network
- Using a serial connection using the serial port on the GbESM

Management Module Setup

The BladeCenter GbE Switch Module is an integral subsystem within the overall BladeCenter system. The BladeCenter chassis includes a management module (MM) as the central element for overall chassis management and control.

You can use the 100-Mbps Ethernet port on the Management Module to configure and manage the GbE Switch Module. The GbE Switch Module communicates with the management module through port MGT1 and port MGT2, which you can access through the 100 Mbps Ethernet port on the management module. The factory default settings will permit *only* management and control access to the switch module through the 10/100 Mbps Ethernet port on the management module, or the built-in serial port. You can use the six external 10/100/1000 Mbps Ethernet ports 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 on the IBM *BladeCenter Documentation* CD for more information).

Factory-Default vs. MM assigned IP Addresses

Each GbE Switch Module 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 10.90.90.9x, where x corresponds to the number of the bay into which the GbE Switch Module 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 GbE Switch Module is installed, as shown in Table 1-1:

Table 1-1 GbE Switch Module 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

Default Gateway

The default Gateway IP address determines where packets with a destination address outside the current subnet should be 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 GbE Switch Module from outside your local network, use the management module to assign a default Gateway address to the GbE Switch Module. Choose **I/O Module Tasks > Management** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

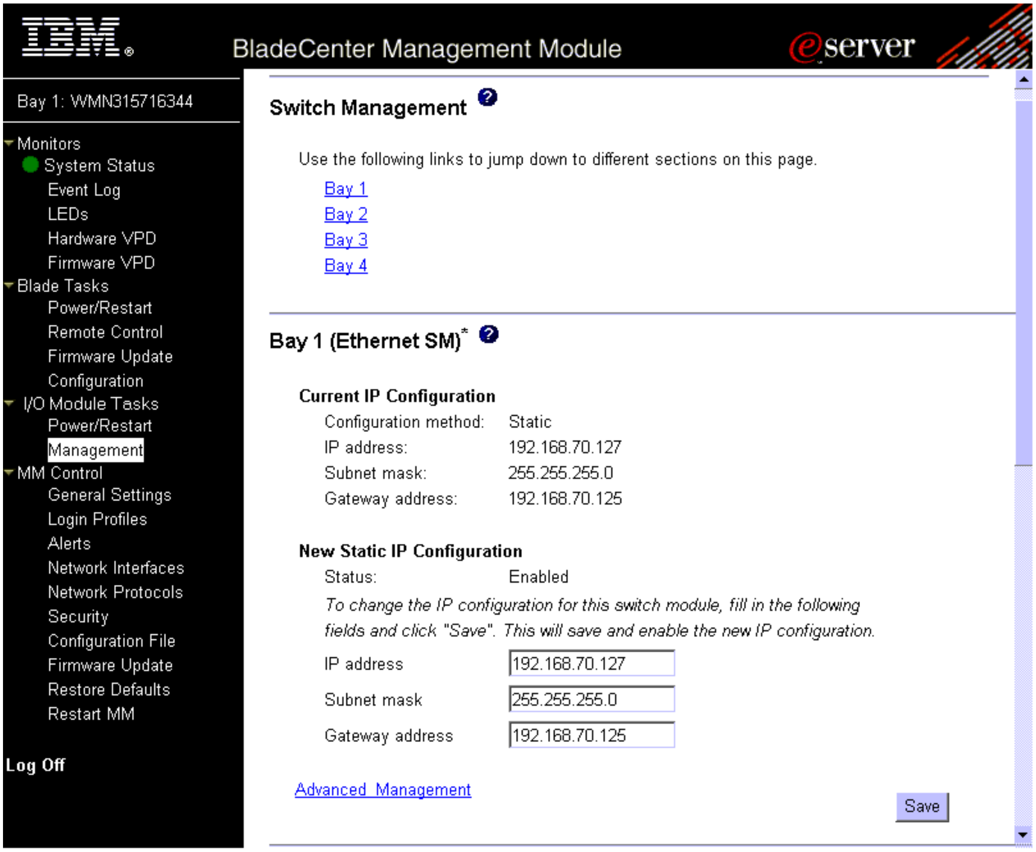
Configuring the Management Module for Switch Access

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* on the IBM *BladeCenter Documentation* CD. The management module provides the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User's Guide* publications on the IBM *BladeCenter Documentation* CD for more information).**

3. **Select** Management **on the** I/O Module Tasks **menu on the left side of the BladeCenter Management Module window. See** Figure 1.



Switch Management

Use the following links to jump down to different sections on this page.

Bay 1
Bay 2
Bay 3
Bay 4

Bay 1 (Ethernet SM)*

Current IP Configuration

Configuration method: Static
IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 192.168.70.125

New Static IP Configuration

Status: Enabled

To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.

IP address: 192.168.70.127
Subnet mask: 255.255.255.0
Gateway address: 192.168.70.125

Advanced Management

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 (when it becomes available)

NOTE – If you change the IP address of the GbE Switch Module, make sure that the GbE Switch Module and the management module both reside on the same subnet.

5. **Enable the following features in the management module (Switch Tasks > Management > Advanced Management):**

   - External Ports
   - External management over all ports (required if you want to access the management network through the six external ports on the GbE Switch Module)

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

NOTE – In the switch management 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, or a Secure Shell session to the GbE Switch Module.

Connecting to the Switch via Telnet

Use the management module to access the GbE Switch Module through Telnet. Choose **I/O Module Tasks > Management** from the navigation pane on the left. Select a bay number and click **Advanced Management > Start Telnet/Web Session > Start Telnet Session**. A Telnet window opens a connection to the Switch Module.

Once that you have configured the GbE Switch Module 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>
```

Running Telnet

Once the IP parameters on the GbE Switch Module 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 22.

Establishing an SSH Connection

Although a remote network administrator can manage the configuration of a GbE Switch Module via Telnet, this method does not provide a secure connection. The SSH (Secure Shell) protocol enables you to securely log into another computer 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 or if another client has just logged in before this client. 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

The following SSH clients have been tested:

- SSH 1.2.23 and SSH 1.2.27 for Linux (freeware)
- SecureCRT 3.0.2 and SecureCRT 3.0.3 (Van Dyke Technologies, Inc.)
- F-Secure SSH 1.1 for Windows (Data Fellows)

NOTE – The Alteon OS implementation of SSH is based on SSH version 1.5 and supports SSH-1.5-1.X.XX. SSH clients of other versions (especially Version 2) will not be supported.

Running SSH

Once the IP parameters are configured and the SSH service is turned on the GbE Switch Module, you can access the command line interface using an SSH connection. The default setting for SSH access is disabled.

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>
```

or, 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 GbE Switch Module. 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 GbE Switch Module. 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 GbE Switch Module. 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 GbE Switch Module. 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 36.

Table 1-2 User Access Levels

User Account	Description and Tasks Performed	Password
User	The User has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	`user`
Operator	The Operator manages all functions of the switch. In addition to SLB Operator functions, the Operator can reset ports or the entire switch.	`oper`

Table 1-2 User Access Levels

User Account	Description and Tasks Performed	Password
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the GbE Switch Module, including the ability to change both the user and administrator passwords.	`admin`

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

Setup Versus 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 (see Chapter 2, “First-Time Configuration”), 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 will not be available.

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see "Menu Basics" on page 41."

Idle Timeout

By default, the switch will disconnect your Telnet session after five 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" on page 153.

CHAPTER 2

First-Time Configuration

To help with the initial process of configuring your switch, the Alteon 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 connection to the switch (see Chapter 1, “Connecting to the Switch”).

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 below.

```
Enter Password:
```

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

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

```
Connected to GbE Switch Module
18:44:05 Wed Jan 3, 2001

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 288.

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

Stopping and Restarting Setup Manually

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
```

Setup Part 1: Basic System Configuration

When Setup is started, the system prompts:

```
"Set Up" will walk you through the configuration of
System Date and Time, BOOTP, Spanning Tree, Port Speed/Mode,
VLANs, and IP interfaces. [type Ctrl-C to abort "Set Up"]
------------------------------------------------------------

Will you be configuring VLANs? [y/n]
```

1. **Enter `y` if you will be configuring VLANs. Otherwise enter `n`.**

   If you decide not to configure VLANs during this session, you can configure them later using the configuration menus, or by restarting the Setup facility. For more information on configuring VLANs, see the *Alteon OS 21.0 Application Guide*.

   Next, the Setup utility prompts you to input basic system information.

2. **Enter the year of the current date at the prompt:**

   ```
   Enter year [2004]:
   ```

   Enter the last two digits of the year as a number from 00 to 99. “00” is considered 2000. To keep the current year, press <Enter>.

NOTE – When the GbE Switch Module is reset, the date and time to revert to default values. Use /cfg/sys/date and /cfg/sys/time to reenter the current date and time.

The system displays the date and time settings:

```
System clock set to 18:55:36 Wed Jan 3, 2004.
```

3. **Enter the month of the current system date at the prompt:**

```
System Date:
Enter month [1]:
```

Enter the month as a number from 1 to 12. To keep the current month, press <Enter>.

4. **Enter the day of the current date at the prompt:**

```
Enter day [3]:
```

Enter the date as a number from 1 to 31. To keep the current day, press <Enter>.

5. **Enter the hour of the current system time at the prompt:**

```
System Time:
Enter hour in 24-hour format [18]:
```

Enter the hour as a number from 00 to 23. To keep the current hour, press <Enter>.

6. **Enter the minute of the current time at the prompt:**

```
Enter minutes [55]:
```

Enter the minute as a number from 00 to 59. To keep the current minute, press <Enter>.

7. **Enter the seconds of the current time at the prompt:**

```
Enter seconds [37]:
```

Enter the seconds as a number from 00 to 59. To keep the current second, press <Enter>.

The system displays the date and time settings:

```
System clock set to 8:55:36 Wed Jan 3, 2001.
```

8. **Turn Spanning Tree Protocol on or off at the prompt:**

```
Spanning Tree:
Current Spanning Tree Group 1 setting: ON
Turn Spanning Tree Group 1 OFF? [y/n]
```

Enter **`y`** to turn off Spanning Tree, or enter **`n`** to leave Spanning Tree on.

Setup Part 2: Port Configuration

NOTE – When configuring port options for your switch, some of the prompts and options may be different.

1. **Select the port to configure, or skip port configuration at the prompt:**

```
Port Config:
Enter port alias or port number (INT1-14, MGT1-2, EXT1-4):
```

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.

If you wish to change settings for individual ports, enter the number of the port you wish to configure. To skip port configuration, press <Enter> without specifying any port and go to "Setup Part 3: VLANs" on page 31.

2. **Configure Gigabit Ethernet port flow parameters.**

If you selected a port that has a Gigabit Ethernet connector, the system prompts:

```
Gig Link Configuration:
Port Flow Control:
Current Port EXT1 flow control setting:    both
Enter new value ["rx"/"tx"/"both"/"none"]:
```

Enter **`rx`** to enable receive flow control, **`tx`** for transmit flow control, **`both`** to enable both, or **`none`** to turn flow control off for the port. To keep the current setting, press <Enter>.

3. **Configure Gigabit Ethernet port autonegotiation mode.**

   If you selected a port that has a Gigabit Ethernet connector, the system prompts:

```
Port Auto Negotiation:
Current Port EXT1 autonegotiation:         on
Enter new value ["on"/"off"]:
```

   Enter **`on`** to enable port autonegotiation, **`off`** to disable it, or press <Enter> to keep the current setting.

4. **If configuring VLANs, enable or disable VLAN tagging for the port.**

   If you have selected to configure VLANs back in Part 1, the system prompts:

```
Port VLAN tagging config (tagged port can be a member of multiple VLANs)
Current TAG support:             disabled
Enter new TAG support [d/e]:
```

   Enter **`d`** to disable VLAN tagging for the port or enter **`e`** to enable VLAN tagging for the port. To keep the current setting, press <Enter>.

5. **The system prompts you to configure the next port:**

```
Enter port alias or port number (INT1-14, MGT1-2, EXT1-4):
```

   When you are through configuring ports, press <Enter> without specifying any port. Otherwise, repeat the steps in this section.

Setup Part 3: VLANs

If you chose to skip VLANs configuration back in Part 1, skip to "Setup Part 4: IP Configuration" on page 32.

1. **Select the VLAN to configure, or skip VLAN configuration at the prompt:**

```
VLAN Config:
Enter VLAN number from 2 to 4095, NULL at end:
```

If you wish to change settings for individual VLANs, enter the number of the VLAN you wish to configure. To skip VLAN configuration, press <Enter> without typing a VLAN number and go to "Setup Part 4: IP Configuration" on page 32.

2. **Enter the new VLAN name at the prompt:**

```
VLAN is newly created.
Pending new VLAN name: VLAN 2
Enter new VLAN name:
```

Entering a new VLAN name is optional. To use the pending new VLAN name, press <Enter>.

3. **Configure jumbo frame support for the VLAN:**

```
VLAN Jumbo Frame Support:
Current jumbo frame support: disabled
Enter new jumbo frame support [d/e]:
```

4. **Enter the VLAN port numbers:**

```
Define Ports in VLAN:
Current VLAN 2:  empty
Enter ports one per line, NULL at end:
```

Enter each port, by port number or port alias, and confirm placement of the port into this VLAN. When you are finished adding ports to this VLAN, press <Enter> without specifying any port.

5. **Configure Spanning Tree Group membership for the VLAN:**

```
Spanning Tree Group membership:
Enter new Spanning Tree Group index [1-16]:
```

6. **The system prompts you to configure the next VLAN:**

```
VLAN Config:
Enter VLAN number from 2 to 4095, NULL at end:
```

Repeat the steps in this section until all VLANs have been configured. When all VLANs have been configured, press <Enter> without specifying any VLAN.

Setup Part 4: IP Configuration

The system prompts for IP parameters.

IP Interfaces

IP interfaces are used for defining subnets to which the switch belongs.

Up to 128 IP interfaces can be configured on the GbE Switch Module. The IP address assigned to each IP interface provide the switch with an IP presence on your network. No two IP interfaces can be on the same IP subnet. The interfaces can be used for connecting to the switch for remote configuration, and for routing between subnets and VLANs (if used).

1. **Select the IP interface to configure, or skip interface configuration at the prompt:**

```
IP Config:

IP interfaces:
Enter interface number: (1-128)
```

If you wish to configure individual IP interfaces, enter the number of the IP interface you with to configure. To skip IP interface configuration, press <Enter> without typing an interface number and go to “Default Gateways” on page 33.

NOTE – Interface 128 is reserved for switch management. If you change the IP address of IF 128, you can lose the connection to the management module. Use the management module to change the IP address of the Gbe Switch Module.

2. **For the specified IP interface, enter the IP address in dotted decimal notation:**

```
Current IP address:     0.0.0.0
Enter new IP address:
```

To keep the current setting, press <Enter>.

3. **At the prompt, enter the IP subnet mask in dotted decimal notation:**

```
Current subnet mask:            0.0.0.0
Enter new subnet mask:
```

To keep the current setting, press <Enter>.

4. **If configuring VLANs, specify a VLAN for the interface.**

This prompt appears if you selected to configure VLANs back in Part 1:

```
Current VLAN:     1
Enter new VLAN:
```

Enter the number for the VLAN to which the interface belongs, or press <Enter> without specifying a VLAN number to accept the current setting.

5. **At the prompt, enter `y` to enable the IP interface, or `n` to leave it disabled**:

```
Enable IP interface? [y/n]
```

6. **The system prompts you to configure another interface:**

```
Enter interface number: (1-128)
```

Repeat the steps in this section until all IP interfaces have been configured. When all interfaces have been configured, press <Enter> without specifying any interface number.

Default Gateways

1. **At the prompt, select a default gateway for configuration, or skip default gateway configuration:**

```
IP default gateways:
Enter default gateway number: (1-132)
```

Enter the number for the default gateway to be configured. To skip default gateway configuration, press <Enter> without typing a gateway number and go to "IP Routing" on page 34.

2. **At the prompt, enter the IP address for the selected default gateway:**

```
Current IP address:      0.0.0.0
Enter new IP address:
```

Enter the IP address in dotted decimal notation, or press <Enter> without specifying an address to accept the current setting.

3. **At the prompt, enter `y` to enable the default gateway, or `n` to leave it disabled:**

```
Enable default gateway? [y/n]
```

4. **The system prompts you to configure another default gateway:**

```
Enter default gateway number: (1-132)
```

Repeat the steps in this section until all default gateways have been configured. When all default gateways have been configured, press <Enter> without specifying any number.

IP Routing

When IP interfaces are configured for the various subnets attached to your switch, IP routing between them can be performed entirely within the switch. This eliminates the need to send inter-subnet communication to an external router device. Routing on more complex networks, where subnets may not have a direct presence on the GbE Switch Module, can be accomplished through configuring static routes or by letting the switch learn routes dynamically.

This part of the Setup program prompts you to configure the various routing parameters.

1. **At the prompt, enable or disable forwarding for IP Routing:**

```
Enable IP forwarding? [y/n]
```

Enter `y` to enable IP forwarding. To disable IP forwarding, enter `n` and proceed to Step 2.To keep the current setting, press <Enter>.

2. **At the prompt, enable or disable the RIP supply:**

```
Enable RIP supply? [y/n]
```

Setup Part 5: Final Steps

1. **When prompted, decide whether to restart Setup or continue:**

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

Enter **y** to restart the Setup utility from the beginning, or **n** to continue.

2. **When prompted, decide whether you wish to review the configuration changes:**

```
Review the changes made? [y/n]
```

Enter **y** to review the changes made during this session of the Setup utility. Enter **n** to continue without reviewing the changes. We recommend that you review the changes.

3. **Next, decide whether to apply the changes at the prompt:**

```
Apply the changes? [y/n]
```

Enter **y** to apply the changes, or **n** to continue without applying. Changes are normally applied.

4. **At the prompt, decide whether to make the changes permanent:**

```
Save changes to flash? [y/n]
```

Enter **y** to save the changes to flash. Enter **n** to continue without saving the changes. Changes are normally saved at this point.

5. **If you do not apply or save the changes, the system prompts whether to abort them:**

```
Abort all changes? [y/n]
```

Enter **y** to discard the changes. Enter **n** to return to the “`Apply the changes?`” prompt.

NOTE – After initial configuration is complete, it is recommended that you change the default passwords as shown in “Setting Passwords” on page 36.

Optional Setup for Telnet Support

NOTE – This step is optional. Perform this procedure only if you are planning on connecting to the GbE Switch Module through a remote Telnet connection.

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

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

2. **Apply and save SNMP and /or telnet configuration(s).**

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

If your network uses Routing Interface Protocol (RIP), enter **y** to enable the RIP supply. Otherwise, enter **n** to disable it. When RIP is enabled, RIP listen is set by default.

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 both the user password and the administrator password, you must login using the administrator password. Passwords cannot be modified from the user command mode.

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
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring 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
```

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

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone (daylight savings)
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     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)
     http     - Enable/disable HTTP (Web) access
     https    - HTTPS Web Access Menu
     wport    - Set HTTP (Web) server port number
     snmp     - Set SNMP access control
     tnet     - Enable/disable Telnet access
     tnport   - Set Telnet server port number
     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 cannot be changed from the user account. Only the administrator has the ability to change 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 GbE Switch Module's 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

- **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 Command 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, performing port mirroring, and enabling or disabling Server Load Balancing functions. 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                up                  print               pwd
lines               verbose             exit                quit
diff                apply               save                revert
ping                traceroute          telnet              history
pushd               popd

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

Table 3-1 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.
`.. 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`	Set the number of lines (n) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed. Set lines to a value of 0 (zero) to disable pagination.
`diff`	Show any pending configuration changes.
`apply`	Apply pending configuration changes.
`save`	Write configuration changes to non-volatile flash memory.

Table 3-1 Description of Global Commands

Command	Action
revert	Remove pending configuration changes between "apply" commands. Use this command to restore configuration parameters set since last "apply" command.
exit or quit	Exit from the command line interface and log out.
ping	Use this command to verify station-to-station connectivity across the network. The format is as follows: **ping** *<host name>* | *<IP address>* [*tries (1-32)> [msec delay*]] [**-m** | **-mgmt** | **-d** | **-data**] Where *IP address* is the hostname or IP address of the device, *tries* (optional) is the number of attempts (1-32), *msec delay* (optional) is the number of milliseconds between attempts. By default, the **-d** or **-data** option for network ports is in effect. If the management port is used, specify the **-m** or **-mgmt** option. The DNS parameters must be configured if specifying hostnames (see "Domain Name System Configuration" on page 249).
traceroute	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **traceroute** *<host name>*| *<IP address>* [*<max-hops (1-32)>* [*msec delay*]] [**-m** | **-mgmt** | **-d** | **-data**] Where *IP address* is the hostname or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-16 devices), and *delay* (optional) is the number of milliseconds for wait for the response. By default, the **-d** or **-data** option for network ports is in effect. If the management port is used, specify the **-m** or **-mgmt** option. As with `ping`, the DNS parameters must be configured if specifying hostnames.
pwd	Display the command path used to reach the current menu.
verbose *n*	Sets the level of information displayed on the screen: `0` =Quiet: Nothing appears except errors—not even prompts. `1` =Normal: Prompts and requested output are shown, but no menus. `2` =Verbose: Everything is shown. When used without a value, the current setting is displayed.
telnet	This command is used to telnet out of the switch. The format is as follows: *<hostname>* | *<IP address>* [port] [**-m** | **-mgmt** | **-d** | **-data**]. Where *IP address* is the hostname or IP address of the device. By default, the **-d** or **-data** option for network ports is in effect. If the management port is used, specify the **-m** or **-mgmt** option.
history	This command brings up the history of the last 10 commands.

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 3-2 Command Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 10 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 10 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 10 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

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/stg/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/st/p
```

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
     l2        - Layer 2 Information Menu
     l3        - Layer 3 Information Menu
     link      - Show link status
     port      - Show port information
     geaport   - Show system port and gea port mapping
     sfp       - Show Fiber External Port SFP status
     dump      - Dump all information
```

The information provided by each menu option is briefly described in Table 4-1 on page 47, with pointers to where detailed information can be found.

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage
`sys` Displays the System Information Menu. For details, see page 49.
`l2` Displays the Layer 2 Information Menu. For details, see page 61.
`l3` Displays the Layer 3 Information Menu. For details, see page 81.

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage
`link` Displays configuration information about each port, including: ■ Port alias ■ Port speed (10, 100, 10/100, or 1000) ■ Duplex mode (half, full, or auto) ■ Flow control for transmit and receive (no, yes, or auto) ■ Link status (up or down) For details, see page 100.
`port` Displays port status information, including: ■ Port alias ■ Whether the port uses VLAN Tagging or not ■ Port VLAN ID (PVID) ■ Port name ■ VLAN membership For details, see page 101.
`geaport` Displays the GbESM port mapping between the two Gigabit Ethernet Aggregators (GEA). For details, see page 102.
`sfp` Displays the status of the Small Form Pluggable (SFP) module on each Fiber External Port. For details, see page 103.
`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

```
[System Menu]
     snmpv3    - SNMPv3 Information Menu
     general   - Show general system information
     log       - Show last 30 syslog messages
     dump      - Dump all system information
```

The information provided by each menu option is briefly described in Table 4-2 on page 49, with pointers to where detailed information can be found.

Table 4-2 System Menu Options (/info/sys)

Command Syntax and Usage
`snmpv3` Displays SNMPv3 Information Menu. To view the menu options, see page 50.
`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 IP interface #1 ■ Hardware version and part number ■ Software image file and version number ■ Configuration name ■ Log-in banner, if one is configured For details, see page 59.
`log` Displays 30 most recent syslog messages. For details, see page 60.
`dump` Dumps all switch information available from the Information Menu (10K or more, depending on your configuration).

/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 4-3 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 51.
view Displays information about view, sub tress, mask and type of view. To view a sample, see page 52.
access Displays View-based Access Control information. To view a sample, see page 53.
group Displays information about the group that includes, the security model, user name, and group name. To view a sample, see page 54.
comm Displays information about the community table information. To view a sample, see page 54.
taddr Displays the Target Address table information. To view a sample, see page 55.

Table 4-3 SNMPv3 information Menu Options (/info/sys/snmpv3)

Command Syntax and Usage
tparam Displays the Target parameters table information. To view a sample, see page 56.
notify Displays the Notify table information. To view a sample, see page 57.
dump Displays all the SNMPv3 information. To view a sample, see page 58.

/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 information like:

- 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
-------------------------------- --------------------------------
admin                            NO AUTH,   NO PRIVACY
adminmd5                         HMAC_MD5, DES PRIVACY
adminsha                         HMAC_SHA, DES PRIVACY
v1v2only                         NO AUTH,   NO PRIVACY
```

Table 4-4 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. Alteon OS 21.0 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
-----------------    ------------------   --------------  --------
org                  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 4-5 SNMPv3 View Table Information Parameters (/info/sys/snmpv3/view)

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

/info/sys/snmpv3/access

SNMPv3 Access Table Information

The access control sub system provides authorization services.

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

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

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

Table 4-6 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          admin                             admin
usm          adminmd5                          admingrp
usm          adminsha                          admingrp
```

Table 4-7 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 4-8 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 4-9 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
```

Table 4-10 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
```

Table 4-11 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 which is used to select entries in the `snmpTargetAddrTable`. Any entry in the `snmpTargetAddrTable` that contains a tag value equal to the value of this entry, is selected. If this entry contains a value of zero length, no entries are selected.

/info/sys/snmpv3/dump

SNMPv3 Dump Information

```
usmUser Table:
User Name                        Protocol
-------------------------------- --------------------------------
admin                            NO AUTH,  NO PRIVACY
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
---------- ------ ------- ---------- ------ ------- -------- ------
admin             usm     noAuthNoPriv exact  org     org     org
v1v2grp          snmpv1  noAuthNoPriv exact  org     org     v1v2only
admingrp          usm     authPriv     exact  org     org     org

vacmViewTreeFamily Table:
View Name            Subtree           Mask            Type
-------------------- ---------------  ------------    --------------
org                  1.3                               included
v1v2only             1.3                               included
v1v2only             1.3.6.1.6.3.15                    excluded
v1v2only             1.3.6.1.6.3.16                    excluded
v1v2only             1.3.6.1.6.3.18                    excluded

vacmSecurityToGroup Table:
Sec Model  User Name                        Group Name
---------- -------------------------------  -----------------------
snmpv1     v1v2only                         v1v2grp
usm        admin                            admin
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/general
General System Information

```
System Information at  0:16:42 Thu Dec  1, 2004
Time zone: No timezone configured

Nortel Networks Layer 2-3 GbE Switch Module

Switch is up 0 days, 0 hours, 16 minutes and 42 seconds.
Last boot:  0:00:47 Thu Dec  1, 2004 (power cycle)

MAC address: 00:11:58:ad:a3:00    IP (If 128) address: 10.90.90.97
Software Version 1.0.0.10 (FLASH image2), factory default configura-
tion.

PCBA Part Number:       317857-A
FAB Number:             EL4512011
Serial Number:          YJ1WDW47N277
Manufacturing Date:
Hardware Revision:      0
PLD Firmware Version:   0.7

Temperature Sensor 1 (Warning):   30.0 C (Warn at 75.0 C/Recover at
70.0 C)
Temperature Sensor 2 (Shutdown):  30.5 C (Warn at 90.0 C/Recover at
80.0 C)
```

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

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- IP address of IP interface #1
- Hardware version and part number
- Software image file and version number

- Configuration name
- Log-in banner, if one is configured

/info/sys/log
Show Last 30 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 that the administrator is being notified of, as shown below.

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

- `DEBUG`: indicates a debut-level message

/info/l2
Layer 2 Menu

```
[Layer 2 Menu]
     fdb      - Forwarding Database Information Menu
     lacp     - Link Aggregation Control Protocol Menu
     8021p    - Show QOS 802.1p information
     8021x    - Show 802.1x information
     stp      - Show STP information
     cist     - Show CIST information
     trunk    - Show Trunk Group information
     vlan     - Show VLAN information
     dump     - Dump all layer 2 information
```

The information provided by each menu option is briefly described in Table 4-12 on page 61, with pointers to where detailed information can be found.

Table 4-12 Layer 2 Menu Options (/info/l2)

Command Syntax and Usage
`fdb` Displays the Forwarding Database Information Menu. For details, see page 63.
`lacp` Displays the Link Aggregation Control Protocol Menu. For details, see page 65.
`8021p` Displays the 802.1p Information Menu. For details, see page 67.
`8021x` Displays the 802.1x Information Menu. For details, see page 69.

Table 4-12 Layer 2 Menu Options (/info/l2)

Command Syntax and Usage
`stg` In addition to seeing if STG is enabled or disabled, you can view the following STG bridge information: ■ Priority ■ Hello interval ■ Maximum age value ■ Forwarding delay ■ Aging time You can also see the following port-specific STG information: ■ Port alias and priority ■ Cost ■ State For details, see page 71.
`cist` Displays Common internal Spanning Tree (CIST) bridge information, including the following: ■ Priority ■ Hello interval ■ Maximum age value ■ Forwarding delay You can also view port-specific CIST information, including the following: ■ Port number and priority ■ Cost ■ State For details, see page 77.
`trunk` When trunk groups are configured, you can view the state of each port in the various trunk groups. For details, see page 79.
`vlan` Displays VLAN configuration information, including: ■ VLAN Number ■ VLAN Name ■ Status ■ Port membership of the VLAN For details, see page 80.
`dump` Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration). If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump commands.

/info/l2/fdb
FDB Information Menu

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

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

NOTE – The master forwarding database supports up to 16K MAC address entries on the MP per switch.

Table 4-13 FDB Information Menu Options (/info/l2/fdb)

Command Syntax and Usage
find *<MAC address>* [*<VLAN>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`. You can also enter the MAC address using the format, `xxxxxxxxxxxx`. For example, `080020123456`.
port *<port number or alias>* Displays all FDB entries for a particular port.
vlan *<VLAN number (1-4095)>* Displays all FDB entries on a single VLAN.
dump Displays all entries in the Forwarding Database. For more information, see page 64.

/info/l2/fdb/dump

Show All FDB Information

```
  MAC address    VLAN  Port Trunk State  Referenced SPs Learned port
----------------- ----  ---- ----- -----  -------------- ------------
00:02:01:00:00:00  300  EXT1        FWD     2             EXT1
00:02:01:00:00:01  300  INT1        FWD     1             INT1
00:02:01:00:00:02  300  INT1        FWD     2             INT1
00:02:01:00:00:03  300  INT7        FWD     1             INT7
00:02:01:00:00:04  300  INT3        FWD     1             INT3
00:02:01:00:00:05  300  INT4        FWD     2             INT4
00:02:01:00:00:06  300  INT6        FWD     2             INT6
00:02:01:00:00:07  300  INT2        FWD     2             INT2
00:02:01:00:00:08  300  INT5        FWD     1 2           INT5
00:02:01:00:00:09  300  INT4        FWD     1 2           INT4
00:02:01:00:00:0a  300  INT3        FWD     1 2           INT3
00:02:01:00:00:0b  300  INT2        FWD     1 2           INT2
00:02:01:00:00:0c  4095 MGT1        FWD     1             MGT1
```

An address that is in the forwarding (FWD) state, means that it has been learned by the switch. When in the trunking (TRK) state, the port field represents the trunk group number. If the state for the port is listed as unknown (UNK), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated, although ports which reference the address as a destination will be listed under “Reference ports.”

If the state for the port is listed as an interface (IF), the MAC address is for a standard VRRP virtual router. If the state is listed as a virtual server (VIP), the MAC address is for a virtual server router—a virtual router with the same IP address as a virtual server.

Clearing Entries from the Forwarding Database

To delete a MAC address from the forwarding database (FDB) or to clear the entire FDB, refer to “Forwarding Database Options” on page 293.

/info/l2/lacp
Link Aggregation Control Protocol menu

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

Use these commands to display LACP status information about each port on a GbE Switch Module.

Table 4-14 Link Aggregation Control Protocol (/info/l2/lacp)

Command Syntax and Usage
aggr Displays detailed information of the LACP aggregator used by the selected port.
port Displays LACP information about the selected port.
dump Displays a summary of LACP information. For details, see page 65.

/info/l2/lacp/dump
Link Aggregation Control Protocol

```
port  lacp  adminkey  operkey  selected  prio  attached  trunk
                                                  aggr
--------------------------------------------------------------
EXT1  active     30       30         y     128      17     19
EXT2  active     30       30         y     128      17     19
EXT3  off        19       19         n     128      --     --
EXT4  off        20       20         n     128      --     --
```

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

- lacp
  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.
- attached aggr
  Displays the aggregator associated with each port.
- trunk
  This value represents the LACP trunk group number.

/info/l2/8021p

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
EXT5        0       0      1
EXT6        0       0      1
```

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

Table 4-15 802.1p 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 4-16 802.1p 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/l2/8021x
802.1x Information

```
System capability : Authenticator
System status     : disabled
Protocol version  : 1
                                   Authenticator     Backend
Port     Auth Mode     Auth Status    PAE State      Auth State
-----  ------------  ------------  --------------  ----------
 INT1  force-auth    authorized    initialize      initialize
*INT2  force-auth    authorized    initialize      initialize
*INT3  force-auth    authorized    initialize      initialize
*INT4  force-auth    authorized    initialize      initialize
*INT5  force-auth    authorized    initialize      initialize
*INT6  force-auth    authorized    initialize      initialize
*INT7  force-auth    authorized    initialize      initialize
*INT8  force-auth    authorized    initialize      initialize
 INT9  force-auth    authorized    initialize      initialize
 INT10 force-auth    authorized    initialize      initialize
*INT11 force-auth    authorized    initialize      initialize
*INT12 force-auth    authorized    initialize      initialize
*INT13 force-auth    authorized    initialize      initialize
*INT14 force-auth    authorized    initialize      initialize
*MGT1  force-auth    authorized    initialize      initialize
*MGT2  force-auth    authorized    initialize      initialize
 EXT1  force-auth    authorized    initialize      initialize
 EXT2  force-auth    authorized    initialize      initialize
*EXT3  force-auth    authorized    initialize      initialize
 EXT4  force-auth    authorized    initialize      initialize
 EXT5  force-auth    authorized    initialize      initialize
 EXT6  force-auth    authorized    initialize      initialize
------------------------------------------------------------------
* - 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 4-17 802.1x Parameter Descriptions

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

/info/l2/stg
Spanning Tree Information

```
Spanning Tree Group 1: On (STP/PVST)
VLANs:  1

Current Root:            Path-Cost  Port Hello MaxAge FwdDel Aging
 8000 00:03:42:fa:3b:80        0       0    2     20      15     300

Parameters:  Priority  Hello  MaxAge  FwdDel  Aging
              32768      2      20      15     300

Port  Priority   Cost     State      Designated Bridge     Des Port
----  --------   ----   ----------  ----------------------  --------
INT1      128     5     FORWARDING   8000-00:03:42:fa:3b:80   32769
INT2      128     5     FORWARDING   8000-00:03:42:fa:3b:80   32770
INT3       128      0      DISABLED
INT4       128      0      DISABLED
INT5       128      0      DISABLED
INT6       128      0      DISABLED
INT7       128      0      DISABLED
INT8       128      0      DISABLED
INT9       128      0      DISABLED
INT10      128      0      DISABLED
INT11     128     10     FORWARDING   8000-00:03:42:fa:3b:80  32779
INT12      128      0      DISABLED
INT13      128      0      DISABLED
INT14      128      0      DISABLED
EXT1       128      0      DISABLED
EXT2       128      0      DISABLED
EXT3       128      0      DISABLED
EXT4       128      0      DISABLED
EXT5       128      0      DISABLED
EXT6       128      0      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 switch software uses the IEEE 802.1d Spanning Tree Protocol (STP). 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:

- Slot number
- Port alias and priority
- Cost
- State

The following table describes the STG parameters.

Table 4-18 Spanning Tree Parameter Descriptions

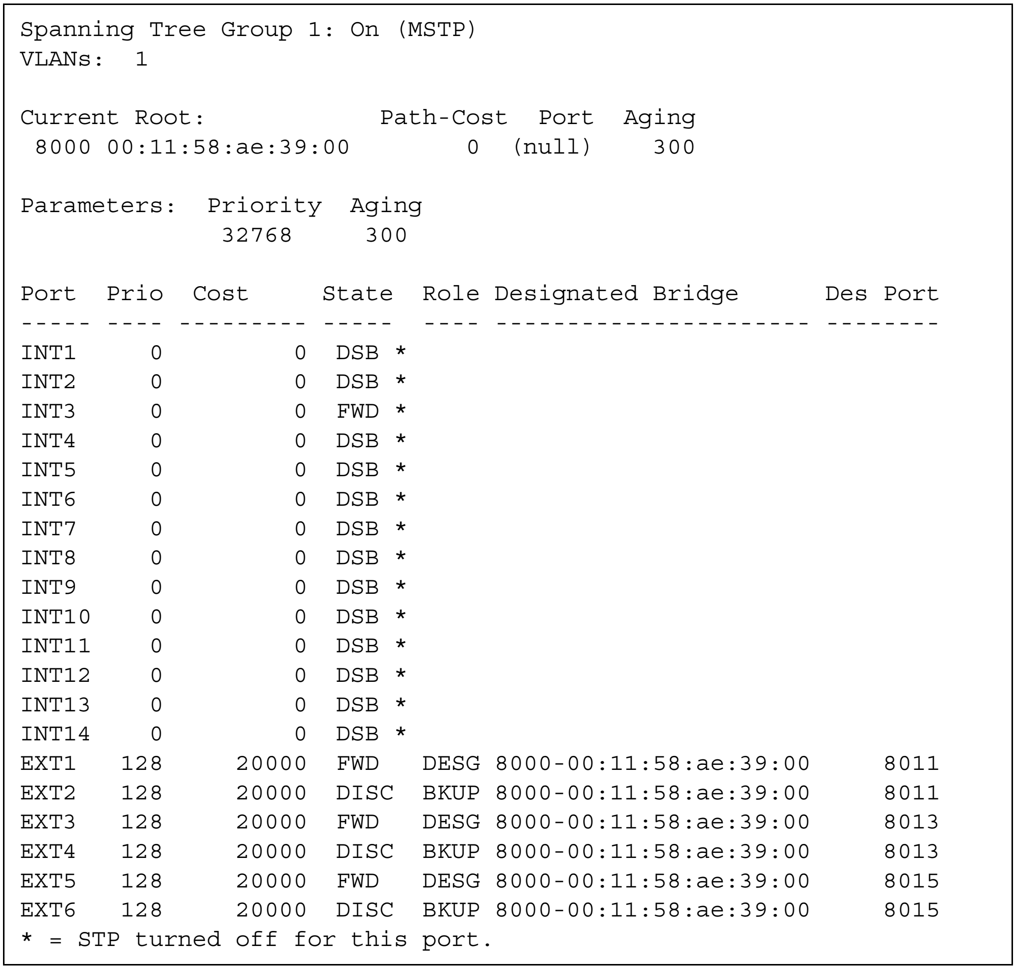
Parameter	Description
`Priority` (bridge)	The bridge priority parameter controls which bridge on the network will become the STG root bridge.
`Hello`	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is 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 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.

Table 4-18 Spanning Tree Parameter Descriptions (Continued)

Parameter	Description
`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 `BLOCKING`, `LISTENING`, `LEARNING`, `FORWARDING`, or `DISABLED`.

/info/l2/stg

RSTP/MSTP Information



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

Current Root:            Path-Cost  Port  Aging
 8000 00:11:58:ae:39:00        0  (null)    300

Parameters:  Priority  Aging
              32768     300

Port  Prio  Cost     State  Role Designated Bridge      Des Port
----- ---- --------- -----  ---- ---------------------- --------
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     20000  FWD   DESG 8000-00:11:58:ae:39:00     8011
EXT2   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00     8011
EXT3   128     20000  FWD   DESG 8000-00:11:58:ae:39:00     8013
EXT4   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00     8013
EXT5   128     20000  FWD   DESG 8000-00:11:58:ae:39:00     8015
EXT6   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00     8015
* = 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 115), you can view RSTP/MSTP bridge information for the Spanning Tree Group, including the following:

- Priority
- Hello interval
- Maximum age value
- Forwarding delay
- Aging time

You can view port-specific RSTP information, including the following:

- Port number and priority
- Cost
- State

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

Table 4-19 Rapid 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 (hex) and MAC address of the root.
`Priority` (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
`Hello`	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
`MaxAge`	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it 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 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.

Table 4-19 Rapid Spanning Tree Parameter Descriptions (Continued)

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

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
              32768      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  DSB *
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    P2P
EXT5   128     20000  FWD   DESG 8000-00:11:58:ae:39:00    8015   2    P2P
EXT6   128     20000  DISC  BKUP 8000-00:11:58:ae:39:00    8015   2    P2P
* = 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 information, including the following:

- Priority
- Maximum age value
- Forwarding delay

You can view port-specific CIST information, including the following:

- Port number and priority
- Cost
- Link type and Port type

The following table describes the CIST parameters.

Table 4-20 Common Internal Spanning Tree Parameter Descriptions

Parameter	**Description**
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
`Priority` (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
`Hello`	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
`MaxAge`	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
`FwdDel`	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
`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.

Table 4-20 Common Internal Spanning Tree Parameter Descriptions

Parameter	Description
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 (hex) 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.

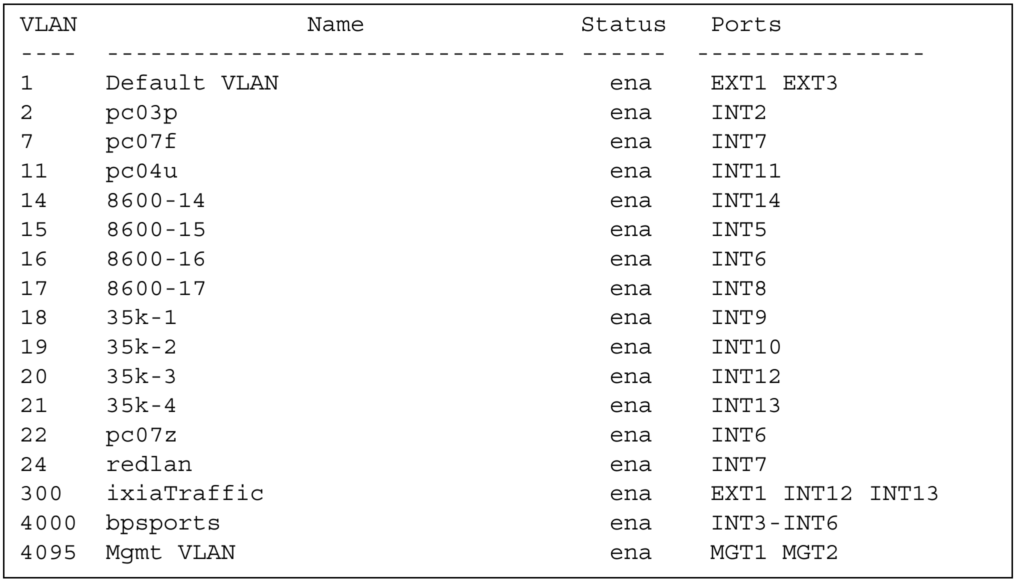
/info/l2/trunk
Trunk Group Information

```
Trunk group 1, failover ena, port state:
  1: STG  1 forwarding
  2: 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   Ports
----  -------------------------------- ------   ----------------
1     Default VLAN                       ena     EXT1 EXT3
2     pc03p                              ena     INT2
7     pc07f                              ena     INT7
11    pc04u                              ena     INT11
14    8600-14                            ena     INT14
15    8600-15                            ena     INT5
16    8600-16                            ena     INT6
17    8600-17                            ena     INT8
18    35k-1                              ena     INT9
19    35k-2                              ena     INT10
20    35k-3                              ena     INT12
21    35k-4                              ena     INT13
22    pc07z                              ena     INT6
24    redlan                             ena     INT7
300   ixiaTraffic                        ena     EXT1 INT12 INT13
4000  bpsports                           ena     INT3-INT6
4095  Mgmt VLAN                          ena     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
- Port membership of the VLAN

/info/l3

Layer 3 Menu

```
[Layer 3 Menu]
     route     - IP Routing Information Menu
     arp       - ARP Information Menu
     bgp       - BGP Information Menu
     ospf      - OSPF Routing Information Menu
     rip       - RIP Routing Information Menu
     ip        - Show IP information
     igmp      - Show IGMP Snooping Multicast Group information
     vrrp      - Show Virtual Router Redundancy Protocol information
     dump      - Dump all layer 3 information
```

The information provided by each menu option is briefly described in Table 4-21 on page 81, with pointers to where detailed information can be found.

Table 4-21 Layer 3 Menu 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 83.

`arp`

Displays the Address Resolution Protocol (ARP) Information Menu. For details, see page 85.

`bgp`

Displays BGP Information Menu. To view menu options, see page 88.

`ospf`

Displays OSPF routing Information Menu. For details, see page 90.

`rip`

Displays Routing Information Protocol Menu. For details, see page 95.

Table 4-21 Layer 3 Menu Options (/info/l3)

Command Syntax and Usage
`ip` Displays IP Information. For details, see page 97. 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 information: Enable status, `lnet` and `lmask` ■ Port status
`igmp` Displays IGMP Information Menu. For details, see page 97.
`vrrp` Displays the VRRP Information Menu. For details, see page 98.
`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

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

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

Table 4-22 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 4-23 on page 84.
`tag fixed|static|addr|rip|ospf|bgp|broadcast|martian|vip` Displays routes of a single tag. For a description of IP routing types, see Table 4-24 on page 85.
`if` *<interface number (1-128)>* Displays routes on a single interface.
`dump` Displays all routes configured in the switch. For more information, see page 83.

/info/l3/route/dump

Show All IP Route Information

```
Status code: * - best
    Destination         Mask          Gateway        Type      Tag    Metr If
 --------------- --------------- --------------- --------- --------- ---- --
* 11.0.0.0        255.0.0.0       11.0.0.1        direct    fixed          211
* 11.0.0.1        255.255.255.255 11.0.0.1        local     addr           211
* 11.255.255.255  255.255.255.255 11.255.255.255  broadcast broadcast     211
* 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
* 12.255.255.255  255.255.255.255 12.255.255.255  broadcast broadcast      12
* 13.0.0.0        255.0.0.0       11.0.0.2        indirect  ospf         2 211
* 47.0.0.0        255.0.0.0       47.133.88.1     indirect  static         24
* 47.133.88.0     255.255.255.0   47.133.88.46    direct    fixed          24
* 172.30.52.223   255.255.255.255 172.30.52.223   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 4-23 IP Routing Type Parameters (/info/l3/route/dump/type)

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 4-24 IP Routing Tag Parameters (info/l3/route/tag)

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 GbE Switch Module.
`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.
`vip`	Indicates a route destination that is a virtual server IP address. VIP routes are needed to advertise virtual server IP addresses via BGP.

/info/l3/arp
ARP Information

```
[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
      dump     - Show all ARP entries
      addr     - Show ARP address list
```

The ARP information includes IP address and MAC address of each entry, address status flags (see Table 4-25 on page 85), VLAN and port for the address, and port referencing information.

Table 4-25 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.

Table 4-25 ARP Information Menu Options (/info/l3/arp)

Command Syntax and Usage
`port` *<port alias or number>* Displays the ARP entries on a single port.
`vlan` *<VLAN number (1-4095)>* Displays the ARP entries on a single VLAN.
`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 87.
`addr` Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.

/info/l3/arp/dump

Show All ARP Entry Information

```
IP address     Flags    MAC address       VLAN  Port   Referenced SPs
--------------- ----- ----------------- ---- ----  ---------------
47.80.22.1            00:e0:16:7c:28:86    1  INT6     empty
47.80.23.243     P    00:03:42:fa:3b:30    1           1 2
47.80.23.245          00:c0:4f:60:3e:c1    1  INT6     empty
190.10.10.1      P    00:03:42:fa:3b:30   10           1 2
```

Referenced ports are the ports that request the ARP entry. So the traffic coming into the referenced ports has the destination IP address. From the ARP entry (the referenced ports), this traffic needs to be forwarded to the egress port (port INT6 in the above example).

NOTE – If you have VMA turned on, the referenced port will be the designated port. If you have VMA turned off, the designated port will be the normal ingress port.

The `Flag` field is interpreted as follows:

Table 4-26 ARP Dump Flag Parameters

Flag	Description
`P`	Permanent entry created for switch IP interface.
`P`	Permanent entry created for virtual server IP address.
`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 Flags
--------------- --------------- ----------------- ---- -----
205.178.18.66   255.255.255.255  00:70:cf:03:20:04        P
205.178.50.1    255.255.255.255  00:70:cf:03:20:06    1
205.178.18.64   255.255.255.255  00:70:cf:03:20:05    1
```

/info/l3/bgp
BGP Information Menu

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

Table 4-27 BGP Peer Information Menu Options

Command Syntax and Usage
peer Displays BGP peer information. See page 88 for a sample output.
summary Displays peer summary information such as AS, message received, message sent, up/down, state. See page 89 for a sample output.
dump Displays the BGP routing table. See page 89 for a sample output.

/info/l3/ip/bgp/peer
BGP Peer information

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

```
BGP Peer Information:

  3: 2.1.1.1         , version 0, TTL 1
    Remote AS: 0, Local AS: 0, Link type: IBGP
    Remote router ID: 0.0.0.0,    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: 0, Holdtime: 0, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 0

  4: 2.1.1.4         , version 0, TTL 1
    Remote AS: 0, Local AS: 0, Link type: IBGP
    Remote router ID: 0.0.0.0,    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: 0, Holdtime: 0, MinAdvTime: 60
    LastErrorCode: unknown(0), LastErrorSubcode: unspecified(0)
    Established state transitions: 0
```

/info/l3/ip/bgp/summary

BGP Summary information

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

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

/info/l3/ip/bgp/dump

Dump BGP Information

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

```
 >> BGP# dump
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network         Next Hop        Metr  LcPrf Wght  Path
   --------------- ---------------  ----- ---- ----- --------------
*> 10.0.0.0         205.178.21.147      1        256 147 148 i
*>i205.178.15.0     0.0.0.0                          0 i
*                   205.178.21.147      1        128 147 i
*> 205.178.17.0     205.178.21.147      1        128 147 i
   13.0.0.0         205.178.21.147      1        256 147 {35} ?

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

/info/l3/ospf
OSPF Information

```
[OSPF Information Menu]
      general - Show general information
      aindex  - Show area(s) information
      if      - Show 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 4-28 OSPF Information Menu options

Command Syntax and Usage
`general` Displays general OSPF information. See page 91 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 [1-128]>* Displays interface information for a particular interface. If no parameter is supplied, it displays information for all the interfaces. See page 92 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 93.
`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 4-28 OSPF Information Menu options

Command Syntax and Usage
routes Displays OSPF routing table. See page 94 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

OSPF Interface Information

```
Ip Address 10.10.12.1, Area 0.0.0.1, Admin Status UP
   Router ID 10.10.10.1, State DR, Priority 1
   Designated Router (ID) 10.10.10.1, Ip Address 10.10.12.1
   Backup Designated Router (ID) 10.10.14.1, Ip Address 10.10.12.2
   Timer intervals, Hello 10, Dead 40, Wait 1663, Retransmit 5,
                Poll interval 0, Transit delay 1
   Neighbor count is 1   If Events 4, Authentication type none
```

/info/l3/ospf/dbase

OSPF Database Information

```
[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 4-29 OSPF Database Information Menu (/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:

a) `asbrsum adv-rtr 20.1.1.1` displays ASBR summary LSAs having the advertising router 20.1.1.1.

b) `asbrsum link_state_id 10.1.1.1` displays ASBR summary LSAs having the link state ID 10.1.1.1.

c) `asbrsum self` displays the self advertised ASBR summary LSAs.

d) `asbrsum` with no parameters displays all the ASBR summary LSAs.

`dbsumm`

Displays the following information about the LS database in a table format:

a) the number of LSAs of each type in each area.

b) the total number of LSAs for each area.

c) the total number of LSAs for each LSA type for all areas combined.

d) the 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`.

Table 4-29 OSPF Database Information Menu (/info/l3/ospf/dbase)

Command Syntax and Usage
`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 Information Route Codes

```
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/rip
Routing Information Protocol Menu

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

Use this menu to view information about the RIP configuration, and statistics.

Table 4-30 Routing Information Protocol Menu (/info/l3/rip)

Command Syntax and Usage
routes Displays RIP routes. For more information, see page 95.
dump *<interface number or zero for all IFs)>* Displays RIP user's configuration. For more information, see page 96.

/info/l3/rip/routes
RIP Routes Information

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

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 learnt through RIP, including the routes that are undergoing garbage collection with metric = 16. This table does not contain directly connected routes and locally configured static routes.

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

RIP User Configuration

```
RIP USER CONFIGURATION :
       RIP on updat 30
       RIP Interface 2 : 102.1.1.1,       enabled
       version 2, listen enabled, supply enabled, default none
       poison disabled, trigg enabled, mcast enabled, metric 1
       auth none,key none
       RIP Interface 3 : 103.1.1.1,       enabled
       version 2, listen enabled, supply enabled, default none
       poison disabled, trigg enabled, mcast enabled, metric 1
```

/info/l3/ip
IP Information

```
Interface information:
  1: 47.80.23.243    255.255.254.0   47.80.23.255,    vlan 1, up
Default gateway information: metric strict
  1: 47.80.22.1,      vlan any,  up
Current IP forwarding settings: ON, dirbr disabled
Current local networks:
Current IP port settings:
  All other ports have forwarding ON
Current network filter settings:
  none
Current route map settings:
Current BGP settings:
  ON, pref 100
Current BGP peer settings:
Current BGP aggr settings:
```

/info/l3/igmp
IGMP Multicast Group Information

```
[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
     dump      - Show all groups
```

Table 4-31 describes the commands used to display information about IGMP groups learned by the switch.

Table 4-31 IGMP Multicast Group Menu Options (/info/l3/igmp)

Command Syntax and Usage
`mrouter` Displays IGMP Multicast Router menu. To view menu options, see page 98.
`find` *<IP address>* Displays a single IGMP multicast group by its IP address.

Table 4-31 IGMP Multicast Group Menu Options (/info/l3/igmp)

Command Syntax and Usage
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.
dump Displays information for all multicast groups.

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

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

Table 4-32 describes the commands used to display information about multicast routers learned through IGMP Snooping.

Table 4-32 IGMP Multicast Router Menu Options (/info/igmp/mrouter)

Command Syntax and Usage
dump Displays information for all multicast groups learned by the switch.

/info/l3/vrrp
VRRP Information

Virtual Router Redundancy Protocol (VRRP) support on GbE Switch Module 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, server
  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, proxy
```

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. 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.
- Server status. The `server` state identifies virtual routers that support Layer 4 services. These are known as virtual *server* routers: any virtual router whose IP address is the same as any configured virtual server IP address.
- Proxy status. The proxy state identifies virtual proxy routers, where the virtual router shares the same IP address as a proxy IP address. The use of virtual proxy routers enables redundant switches to share the same IP address, minimizing the number of unique IP addresses that must be configured.

/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      down
 EXT1    17       any      any     yes     yes       up
 EXT2    18       any      any     yes     yes       up
 EXT3    19       any      any     yes     yes       up
 EXT4    20       any      any     yes     yes       up
 EXT5    19       any      any     yes     yes       up
 EXT6    20       any      any     yes     yes       up
```

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

Use this command to display link status information about each port on an GbE Switch Module slot, including:

- Port alias
- Port speed (10, 100, 10/100, or 1000)
- Duplex mode (half, full, any, or auto)
- Flow control for transmit and receive (no, yes, or auto)
- Link status (up or down)

/info/port
Port Information

```
Alias   Port   Tag   FAST    PVID       NAME                VLAN(s)
-----   ----   ---   ----    ----   --------------   -----------------
INT1       1    y     n         1   INT1                  1 4095
INT2       2    y     n         1   INT2                  1 4095
INT3       3    y     n         1   INT3                  1 4095
INT4       4    y     n         1   INT4                  1 4095
INT5       5    y     n         1   INT5                  1 4095
INT6       6    y     n         1   INT6                  1 4095
INT7       7    y     n         1   INT7                  1 4095
INT8       8    y     n         1   INT8                  1 4095
INT9       9    y     n         1   INT9                  1 4095
INT10     10    y     n         1   INT10                 1 4095
INT11     11    y     n         1   INT11                 1 4095
INT12     12    y     n         1   INT12                 1 4095
INT13     13    y     n         1   INT13                 1 4095
INT14     14    y     n         1   INT14                 1 4095
MGT1      15    y     n      4095   MGT1               4095
MGT2      16    y     n      4095   MGT2               4095
EXT1      17    n     n         1   EXT1                  1
EXT2      18    n     n         1   EXT2                  1
EXT3      19    n     n         1   EXT3                  1
EXT4      20    n     n         1   EXT4                  1
EXT5      20    n     n         1   EXT5                  1
EXT6      20    n     n         1   EXT6                  1
```

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
- Whether the port uses VLAN tagging or not (`y` or `n`)
- Port VLAN ID (PVID)
- Port name
- VLAN membership
- Whether the port is configured for Fast Port Fowarding

/info/geaport
Logical Port to GEA Port Mapping

```
Alias  Logical Port  GEA Port(0-based)  GEA Unit
-----  ------------  -----------------  ---------
INT1         1               3                0
INT2         2               2                0
INT3         3              11                1
INT4         4              10                1
INT5         5               9                1
INT6         6               8                1
INT7         7               7                1
INT8         8               6                1
INT9         9               1                1
INT10       10               0                1
INT11       11               3                1
INT12       12               2                1
INT13       13               5                1
INT14       14               4                1
MGT1        15               1                0
MGT2        16               6                0
EXT1        17              10                0
EXT2        18               9                0
EXT3        19               8                0
EXT4        20               7                0
EXT5        21               5                0
EXT6        22               4                0
```

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 display correlates the port alias to logical port number, and shows the GEA unit on which each port resides.

/info/sfp

Fiber Port SFP Status

```
Port  TX-Enable  RX-Signal  TX-Fault
----  ---------  ---------  --------
EXT1  enabled    LOST       none
EXT2  DISABLED   LOST       none   <= SFP NOT APPROVED
EXT3  enabled    LOST       none
EXT4  enabled    LOST       none
EXT5  enabled    LOST       none
EXT6  enabled    LOST       none
```

This command displays the status of the Small Form Pluggable (SFP) module on each Fiber External Port.

/info/dump

Information Dump

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

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

CHAPTER 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
     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
     dump      - Dump all stats
```

Table 5-1 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 107.
`l2` Displays the Layer 2 Stats Menu. To view menu options, see page 119.
`l3` Displays the Layer 3 Stats Menu. To view menu options, see page 121.
`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 135.
`acl` Displays ACL menu. To view menu options, see page 139.
`snmp` Displays SNMP statistics. See page 141 for sample output.
`ntp` *<clear>* Displays Network Time Protocol (NTP) Statistics. See page 145 for a sample output and a description of NTP Statistics. You can execute the `clear` command option to delete all statistics.
`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 147.

`/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
     brg      - Show bridging ("dot1") stats
     ether    - Show Ethernet ("dot3") stats
     if       - Show interface ("if") stats
     ip       - Show Internet Protocol ("IP") stats
     link     - Show link stats
     clear    - Clear all port stats
```

Table 5-2 Port Statistics Menu Options (/stats/port)

Command Syntax and Usage
`8021x` Displays IEEE 802.1x statistics for the port. See page 112 for sample output.
`brg` Displays bridging (“dot1”) statistics for the port. See page 112 for sample output.
`ether` Displays Ethernet (“dot1”) statistics for the port. See page 113 for sample output.
`if` Displays interface statistics for the port. See page 116 for sample output.
`ip` Displays IP statistics for the port. See page 118 for sample output.
`link` Displays link statistics for the port. See page 119 for sample output.
`clear` This command clears all the statistics on the 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 5-3 802.1x 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.

Table 5-3 802.1x Authenticator Statistics of a Port (/stats/port/8021x)

Statistics	Description
`lastEapolFrame-Source`	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 5-4 802.1x 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.
`authEapLogoffsWhileConnecting`	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.

Table 5-4 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
`authEntersAuthenticating`	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.
`authSuccessesWhileAuthenticating`	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.
`authTimeoutsWhileAuthenticating`	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.
`authFailWhileAuthenticating`	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.
`authReauthsWhileAuthenticating`	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
`authEapStartsWhileAuthenticating`	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.
`authEapLogoffWhileAuthenticating`	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.
`authReauthsWhileAuthenticated`	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
`authEapStartsWhileAuthenticated`	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.
`authEapLogoffWhileAuthenticated`	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.
`backendAccessChallenges`	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.

Table 5-4 802.1x Authenticator Diagnostics of a Port (/stats/port/8021x)

Statistics	Description
`backendOtherRequestsToSupplicant`	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.
`backendNonNakResponsesFromSupplicant`	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.
`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>*/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
dot1BasePortDelayExceededDiscards:          NA
dot1BasePortMtuExceededDiscards:            NA
dot1StpPortForwardTransitions:               0
```

Table 5-5 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.
dot1BasePortDelay ExceededDiscards	The number of frames discarded by this port due to excessive transit delay through the bridge. It is incriminated by both transparent and source route bridges.
dot1BasePortMtu ExceededDiscards	The number of frames discarded by this port due to an excessive size. It is incremented by both transparent and source route bridges.
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 INT1:
dot3StatsAlignmentErrors:                      0
dot3StatsFCSErrors:                            0
dot3StatsSingleCollisionFrames:                0
dot3StatsMultipleCollisionFrames:              0
dot3StatsSQETestErrors:                       NA
dot3StatsDeferredTransmissions:                0
dot3StatsLateCollisions:                       0
dot3StatsExcessiveCollisions:                  0
dot3StatsInternalMacTransmitErrors:           NA
dot3StatsCarrierSenseErrors:                   0
dot3StatsFrameTooLongs:                        0
dot3StatsInternalMacReceiveErrors:             0
dot3CollFrequencies [1-15]:                   NA
```

Table 5-6 Ethernet Statistics for 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 5-6 Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
`dot3StatsSingleCollisionFrames`	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.
`dot3StatsMultipleCollisionFrames`	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.
`dot3StatsSQETestErrors`	A count of times that the SQE TEST ERROR message is generated by the PLS sub layer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
`dot3StatsDeferredTransmissions`	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
`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.
`dot3StatsInternalMacTransmitErrors`	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 5-6 Ethernet Statistics for Port (/stats/port/ether)

Statistics	Description
`dot3StatsCarrierSenseErrors`	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
`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.
`dot3StatsInternalMacReceiveErrors`	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.
`dot3CollFrequencies`	A count of individual MAC frames for which the transmission (successful or otherwise) on a particular interface occurs after the frame has experienced exactly the number of collisions in the associated `dot3CollCount` object. For example, a frame which is transmitted on interface 77 after experiencing exactly 4 collisions would be indicated by incrementing only `dot3CollFrequencies`. 77.4. No other instance of `dot3CollFrequencies` would be incremented in this example.

/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
Discards:                          0                      0
Errors:                            0                  21187
```

Table 5-7 Interface Statistics for 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.
`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.

Table 5-7 Interface Statistics for Port (/stats/port/if)

Statistics	Description
`ifInUnknownProtos`	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing, the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface which does not support protocol multiplexing, this counter will always be 0.
`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`.
`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.

```
IP statistics for port INT1:
ipInReceives:              0
ipInAddrErrors:            0   ipForwDatagrams:         0
ipInUnknownProtos:         0   ipInDiscards:            0
ipInDelivers:              0
ipTtlExceeds:              0
ipLANDattacks:             0
```

Table 5-8 Interface Protocol Statistics (/stats/port/ip)

Statistics	Description
`ipInReceives`	The total number of input datagrams received from interfaces, including those received in error.
`ipInAddrErrors`	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
`ipForwDatagrams`	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
`ipInUnknownProtos`	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
`ipInDiscards`	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
`ipInDelivers`	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
`ipTtlExceeds`	The number of IP datagram for which an `ICMP TTL exceeded` message was sent.

/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 5-9 Link Statistics (/stats/port/link)

Statistics	Description
`linkStateChange`	The total number of link state changes.

/stats/l2

Layer 2 Statistics Menu

```
[Layer 2 Statistics Menu]
     fdb      - Show FDB stats
     lacp     - Show LACP stats
```

Table 5-10 Statistics Menu Options (/stats/l2)

Command Syntax and Usage
`fdb` Displays FDB statistics. See page 120 for sample output.
`lacp` *<port alias or number>* Displays Link Aggregation Control Protocol (LACP) statistics. See page 121 for sample output.

/stats/l2/fdb
FDB Statistics

```
FDB statistics:
 current:               83   hiwat:                855
 max:                16384   hash:               16384
```

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 5-11 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.
`max`	Maximum number of FDB entries
`hash`	Number of hash table entries in the Forwarding Database.

/stats/l2/lacp *<port alias or number>*
LACP Statistics

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

/stats/l3
Layer 3 Statistics Menu

```
[Layer 3 Statistics Menu]
     ip        - Show IP stats
     route     - Show route stats
     arp       - Show ARP stats
     icmp      - Show ICMP stats
     if        - Show IP interface ("if") stats
     tcp       - Show TCP stats
     udp       - Show UDP stats
     igmp      - Show IGMP stats
     vrrp      - Show VRRP stats
     rip       - Show RIP stats
     clrigmp   - Clear IGMP stats
     ifclear   - Clear IP interface ("if") stats
     ipclear   - Clear IP stats
     dump      - Dump layer 3 stats
```

Table 5-12 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
`ip` Displays IP statistics. See page 123 for sample output.
`route` Displays route statistics. See page 125 for sample output.
`arp` Displays Address Resolution Protocol (ARP) statistics. See page 127 for sample output.
`icmp` Displays ICMP statistics. See page 127 for sample output.
`if` *<interface number (1-128)>* Displays IP interface statistics. See page 129 for sample output.
`tcp` Displays TCP statistics. See page 131 for sample output.
`udp` Displays UDP statistics. See page 132 for sample output.
`igmp` Displays IGMP statistics. See page 127 for sample output.
`vrrp` When virtual routers are configured, you can display the following protocol statistics for VRRP: ■ Advertisements received (`vrrpInAdvers`) ■ Advertisements transmitted (`vrrpOutAdvers`) ■ Advertisements received, but ignored (`vrrpBadAdvers`) See page 134 for sample output.
`rip` Displays Routing Information Protocol (RIP) statistics. See page 135 for sample output.
`clrigmp` Clears IGMP statistics.
`ifclear` Clears IP interface statistics. Use this command with caution as it will delete all the IP interface statistics.
`ipclear` Clears IP statistics. Use this command with caution as it will delete all the IP statistics.

Table 5-12 Statistics Menu Options (/stats/l3)

Command Syntax and Usage
`dump` Dumps all Layer 3 statistics. Use this command to gather data for tuning and debugging switch performance. If you want to capture dump data to a file, set your communication software on your workstation to capture session data prior to issuing the dump command.

/stats/l3/ip
IP 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 5-13 IP 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.

Table 5-13 IP Statistics (stats/l3/ip)

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

Table 5-13 IP Statistics (stats/l3/ip)

Statistics	Description
`ipFragOKs`	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
`ipFragFails`	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their `Don't Fragment` flag was set.
`ipFragCreates`	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
`ipRoutingDiscards`	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
`ipDefaultTTL`	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
`ipReasmTimeout`	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

/stats/l3/route
Route Statistics

```
Route statistics:
ipRoutesCur:                7   ipRoutesHighWater:          7
ipRoutesMax:             1024

RIP statistics:
ripInPkts:                  0   ripOutPkts:                 0
ripBadPkts:                 0   ripRoutesAgedOut:           0

BGP statistics:
bgpInPkts:                  0   bgpOutPkts:                 0
bgpBadPkts:                 0   bgpSessFailures:            0
bgpRoutesAdded:             0   bgpRoutesRemoved:           0
bgpRoutesCur:               0   bgpRoutesFailed:            0
bgpRoutesIgnored:           0   bgpRoutesFiltered:          0
```

Table 5-14 Route Statistics (/stats/l3/route)

Statistics	Description
`ipRoutesCur`	The total number of outstanding routes in the route table.
`ipRoutesHighWater`	The highest number of routes ever recorded in the route table.
`ipRoutesMax`	The maximum number of routes that are supported.
`RIP statistics:`	
`ripInPkts`	The total number of good RIP advertisement packets received.
`ripOutPkts`	The total number of RIP advertisement packets sent.
`ripBadPkts`	The total number of RIP advertisement packets received that were dropped.
`ripRoutesAgedOut`	The total number of routes learned via RIP that has aged out.
`BGP statistics:`	
`bgpInPkts`	The total number of BGP packets received.
`bgpOutPkts`	The total number of BGP packets sent.
`bgpBadPkts`	The total number of BGP packets dropped.
`bgpSessFailures`	The total number of failed sessions.
`bgpRoutesAdded`	The total number of routes that were added to the routing table.
`bgpRoutesRemoved`	The total number of routes that were removed from the routing table.
`bgpRoutesCur`	The total number of current BGP routes.
`bgpRoutesFailed`	The total number of BGP routes that failed to add in the routing table.
`bgpRoutesIgnored`	The total number of routes ignored because the peer was not connected locally or multihop was not configured.
`bgpRoutesFiltered`	The total number of routes dropped by the filter.

/stats/l3/arp
ARP statistics

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

```
ARP statistics:
arpEntriesCur:               3  arpEntriesHighWater:          4
arpEntriesMax:            4096
```

Table 5-15 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/icmp
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 5-16 ICMP Statistics (/stats/l3/icmp)

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

Table 5-16 ICMP Statistics (/stats/l3/icmp)

Statistics	Description
`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.

`/stats/l3/if` *<interface number>* Interface Statistics

```
IP interface 1 statistics:
ifInOctets:          48948386   ifInUcastPkts:         220553
ifInNUCastPkts:        167895   ifInDiscards:               0
ifInErrors:                 0   ifInUnknownProtos:          0
ifOutOctets:         27100789   ifOutUcastPkts:        441938
ifOutNUcastPkts:       218652   ifOutDiscards:              0
ifOutErrors:                0   ifStateChanges              1
```

Table 5-17 Interface Statistics (/stats/l3/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.
`ifInNUCastPkts`	The number of packets, delivered by this sub-layer to a higher (sub-layer), which were addressed to a multicast or broadcast address at this sub-layer. This object is deprecated in favor of `ifInMulticastPkts` and `ifInBroadcastPkts`.

Table 5-17 Interface Statistics (/stats/l3/if)

Statistics	Description
`ifInDiscards`	The number of inbound packets that 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.
`ifInUnknownProtos`	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface which does not support protocol multiplexing, this counter will always be 0.
`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.
`ifOutNUcastPkts`	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is deprecated in favor of `ifOutMulticastPkts` and `ifOutBroadcastPkts`.
`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.
`ifStateChanges`	The number of times an interface has transitioned from either down to up or from up to down.

/stats/l3/tcp
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 5-18 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.

Table 5-18 TCP Statistics (/stats/l3/tcp)

Statistics	Description
`tcpEstabResets`	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
`tcpInSegs`	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
`tcpOutSegs`	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
`tcpRetransSegs`	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
`tcpInErrs`	The total number of segments received in error (for example, bad TCP `checksums`).
`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.

/stats/l3/udp
UDP Statistics

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

Table 5-19 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.

/stats/l3/igmp
IGMP Statistics

```
IGMP Snoop vlan 1 statistics:
------------------------------------------------------------------
rxIgmpValidPkts:             0   rxIgmpInvalidPkts:            0
rxIgmpGenQueries:            0   rxIgmpGrpSpecificQueries:     0
rxIgmpLeaves:                0   rxIgmpReports:                0
txIgmpReports:               0   txIgmpGrpSpecificQueries:     0
txIgmpLeaves:                0
Current Groups:              0   Current M-cast Routers:       1
```

This menu option enables you to display statistics about the use of the IGMP Multicast Groups.

IGMP statistics are described in the following table:

Table 5-20 IGMP Statistics (/stats/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
`rxIgmpGrpSpecificQueries`	Total number of Membership Query packets received from specific groups
`rxIgmpLeaves`	Total number of Leave requests received
`rxIgmpReports`	Total number of Membership Reports received
`txIgmpReports`	Total number of Membership reports transmitted
`txIgmpGrpSpecificQueries`	Total number of Membership Query packets transmitted to specific groups
`txIgmpLeaves`	Total number of Leave messages transmitted
`Current Groups`	Total number of active IGMP groups learned through IGMP Snooping
`Current M-Cast Routers`	Total number of static Multicast Routers configured on the switch

/stats/l3/vrrp
VRRP Statistics

Virtual Router Redundancy Protocol (VRRP) support on the GbE Switch Module 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 following protocol statistics for VRRP:

- Advertisements received (`vrrpInAdvers`)
- Advertisements transmitted (`vrrpOutAdvers`)
- Advertisements received, but ignored (`vrrpBadAdvers`)

The statistics for the VRRP LAN are displayed:

```
VRRP statistics:
vrrpInAdvers:                   0   vrrpBadAdvers:              0
vrrpOutAdvers:                  0
```

Table 5-21 VRRP Statistics (/stats/l3/vrrp)

Statistics	Description
`vrrpInAdvers`	The total number of 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.

/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

```
[MP-specific Statistics Menu]
      pkt     - Show Packet stats
      tcb     - Show All TCP control blocks in use
      ucb     - Show All UDP control blocks in use
      cpu     - Show CPU utilization
      mem     - Show memory stats
```

Table 5-22 Management Processor Statistics Menu Options (/stats/mp)

Command Syntax and Usage
pkt Displays packet statistics, to check for leads and load. To view a sample output and a description of the stats, see page 136.
tcb Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 137.
ucb Displays all UDP control blocks that are in use. To view a sample output, see page 137.

Table 5-22 Management Processor Statistics Menu Options (/stats/mp)

Command Syntax and Usage
sfd Displays all Socket File Descriptors that are in use. To view a sample output, see page 138.
cpu Displays CPU utilization for periods of up to 1, 4, and 64 seconds. To view a sample output and a description of the stats, see page 138.
mem Displays memory statistics.

/stats/mp/pkt

MP Packet Statistics

```
Packet counts:
 allocs:        1166996     frees:                     1166996
 mediums:             0     mediums hi-watermark:            7
 smalls:              0     smalls hi-watermark:             7
 failures:            0
```

Table 5-23 Packet Statistics (/stats/mp/pkt)

Statistics	Description
`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.
`mediums`	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
`smalls`	Total number of packet allocations with size less than 128 bytes from 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.
`frees`	Total number of packets freed from the packet buffer pool by the TCP/IP protocol stack.
`mediums hi-water-mark`	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

Table 5-23 Packet Statistics (/stats/mp/pkt)

Statistics	Description
`smalls 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.

/stats/mp/tcb

TCP Statistics

```
All TCP allocated control blocks:
10ad41e8:  0.0.0.0             0 <=> 0.0.0.0           80  listen
10ad5790:  47.81.27.5       1171 <=> 47.80.23.243      23  established
```

Table 5-24 MP Specified TCP Statistics (/stats/mp/tcb)

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

/stats/mp/ucb

UCB Statistics

```
All UDP allocated control blocks:
  161:  listen
```

/stats/mp/sfd

MP-Specific SFD Statistics

```
All Socket FD allocated:
max_fdi=2
fdi=0 fd=15 pfdi=-1
10c27fd8: 0.0.0.0           0<=>47.133.108.161 80  listen TCP server
fdi=1 fd=16 pfdi=-1
10b9564c: 0.0.0.0           0<=>47.133.108.161 23 listen TCP server
fdi=2 fd=17 pfdi=1
10c27c78: 47.129.153.150 5341<=>47.133.108.161 23 accept TCP  server
```

/stats/mp/cpu

CPU Statistics

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

```
CPU utilization:
cpuUtil1Second:            53%
cpuUtil4Seconds:           54%
cpuUtil64Seconds:          54%
```

Table 5-25 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.

/stats/acl
ACL Statistics

```
[ACL Menu]
     acl      - Display ACL stats
     meter    - Display ACL metering stats
     dump     - Display all available ACL stats
     clracl   - Clear ACL stats
     clrmeter - Clear ACL metering stats
```

Table 5-26 Management Processor Statistics Menu Options (/stats/acl)

Command Syntax and Usage
`acl` *<1-4096>* Displays the Access Control List Statistics for a specific ACL. For details, see page 140.
`meter` *<1-127>* Displays statistics for a specific ACL Meter. For details, see page 140.
`dump` Displays all ACL statistics.
`clracl` Clears all ACL statistics.
`clrmeter` Clears all ACL metering statistics.

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

ACL Statistics

This option displays statistics for the selected ACL.

```
Hits for ACL 1, port EXT1:              26057515
Hits for ACL 2, port EXT1:              26057497
```

/stats/acl/meter *<meter number>*

ACL Meter Statistics

This option displays statistics of the selected ACL meter.

```
Meters for ACL Group 1, Port EXT1: Out of profile:  0
Meters for ACL Group 2, Port EXT1: Out of profile:  0
```

/stats/snmp
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

SNMPv3 Statistics:
snmpUnknownSecurityModels:             0
snmpInvalidMsgs:                       0
snmpUnknownPDUHandlers:                0
snmpUnknownContexts:                   0
snmpUnavailableContexts:               0
usmStatsUnsupportedSecLevels:          0
usmStatsNotInTimeWindows:              0
usmStatsUnknownUserNames:              2
usmStatsUnknownEngineIDs:              2
usmStatsWrongDigests:                  0
usmStatsDecryptionErrors:              0
```

Table 5-27 SNMP Statistics (/stats/snmp)

Statistics	Description
`snmpInPkts`	The total number of Messages delivered to the SNMP entity from the transport service.

Table 5-27 SNMP Statistics (/stats/snmp)

Statistics	Description
`snmpInBadVersions`	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
`snmpInBadC'tyNames`	The total number of SNMP Messages delivered to the SNMP entity which used an SNMP community name not known to the said entity (the switch).
`snmpInBadC'tyUses`	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.
`snmpInASNParseErrs`	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
`snmpEnableAuth Traps`	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.

Table 5-27 SNMP Statistics (/stats/snmp)

Statistics	Description
`snmpInGenErrs`	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.
`snmpInTotalReqVars`	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get-Request and Get-Next Protocol Data Units (PDUs).
`snmpInTotalSetVars`	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
`snmpInGetRequests`	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`snmpInGetNexts`	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
`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 5-27 SNMP Statistics (/stats/snmp)

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.
`snmpOutGet Responses`	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.
`SNMPv3 Statistics:`	
`snmpUnknownSecurityModels`	The total number of packets received by the SNMP engine which were dropped because they referenced a `securityModel` that was not known to or supported by the SNMP engine.
`snmpInvalidMsgs`	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.
`snmpUnknownPDUHandlers`	The total number of packets received by the SNMP engine which were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the `pduType`, for example, no SNMP application had registered for the proper combination of the `contextEngineID` and the `pduType`.
`snmpUnknownContexts`	The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unavailable.
`snmpUnavailableContexts`	The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unknown.

Table 5-27 SNMP Statistics (/stats/snmp)

Statistics	Description
`usmStatsUnsupportedSecLevels`	The total number of packets received by the SNMP engine which were dropped because they requested a `securityLevel` that was unknown to the SNMP engine or otherwise unavailable.
`usmStatsNotInTimeWindows`	The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
`usmStatsUnknownUserNames`	The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
`usmStatsUnknownEngineIDs`	The total number of packets received by the SNMP engine which were dropped because they referenced an `snmpEngineID` that was not known to the SNMP engine.
`usmStatsWrongDigests`	The total number of packets received by the SNMP engine which were dropped because they didn't contain the expected digest value.
`usmStatsDecryptionErrors`	The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

/stats/ntp
NTP Statistics

Alteon 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
        Last update based on response from primary server.
        Last update time: 18:04:16 Tue Jul 13, 2004
        Current system time: 18:55:49 Tue Jul 13, 2004
```

Table 5-28 NTP Statistics Parameters (/stats/ntp)

Field	Description
`Primary Server`	**Requests Sent:** The total number of NTP requests the switch sent to the primary NTP server to synchronize time. **Responses Received:** The total number of NTP responses received from the primary NTP server. **Updates:** The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Secondary Server	**Requests Sent:** The total number of NTP requests the switch sent to the secondary NTP server to synchronize time. **Responses Received:** The total number of NTP responses received from the secondary NTP server. **Updates:** The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last update based on response from primary server	Last update of time on the switch based on either primary or secondary NTP response received.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The switch system time when the command `/stats/ntp` was issued.

NOTE – You can issue `/stats/ntp/clear` command to delete all statistics.

/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 6

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
     l2        - Layer 2 Menu
     l3        - Layer 3 Menu
     qos       - QOS Menu
     acl       - Access Control List Menu
     pmirr     - Port Mirroring 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
```

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage
`sys` Displays the System Configuration Menu. To view menu options, see page 153.
`port` *<port alias or number>* Displays the Port Configuration Menu. To view menu options, see page 180.
`l2` Displays the Layer 2 Configuration Menu. To view menu options, see page 189.

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage
`l3` Displays the Layer 3 Configuration Menu. To view menu options, see page 213.
`qos` Displays the Quality of Service Configuration Menu. To view menu options, see page 261.
`acl` Displays the ACL Configuration Menu. To view menu options, see page 264.
`pmirr` Displays the Mirroring Configuration Menu. To view menu options, see page 271.
`setup` Step-by-step configuration set-up of the switch. For details, see page 274.
`dump` Dumps current configuration to a script file. For details, see page 274.
`ptcfg` *<host name or IP address of TFTP server>* *<filename on host>* Backs up current configuration to TFTP server. For details, see page 275.
`gtcfg` *<host name or IP address of TFTP server>* *<filename on host>* Restores current configuration from TFTP server. For details, see page 275.

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 GbE Switch Module.

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 288.

/cfg/sys
System Configuration

```
[System Menu]
     syslog   - Syslog Menu
     sshd     - SSH Server Menu
     radius   - RADIUS Authentication Menu
     tacacs+  - TACACS+ Authentication Menu
     ntp      - NTP Server Menu
     ssnmp    - System SNMP Menu
     access   - System Access Menu
     date     - Set system date
     time     - Set system time
     timezone - Set system timezone (daylight savings)
     idle     - Set timeout for idle CLI sessions
     notice   - Set login notice
     bannr    - Set login banner
     hprompt  - Enable/disable display hostname (sysName) in CLI prompt
     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 6-2 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`syslog` Displays the Syslog Menu. To view menu options, see page 155.
`sshd` Displays the SSH Server Menu. To view menu options, see page 156.
`radius` Displays the RADIUS Authentication Menu. To view menu options, see page 157.
`tacacs+` Displays the TACACS+ Authentication Menu. To view menu options, see page 158
`ntp` Displays the Network Time Protocol (NTP) Server Menu. To view menu options, see page 160.
`ssnmp` Displays the System SNMP Menu. To view menu options, see page 162.

Table 6-2 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`access` Displays the System Access Menu. To view menu options, see page 175.
`date` Prompts the user for the system date. The date reverts to its default value when the switch is reset.
`time` Configures the system time using a 24-hour clock format. The time reverts to its default value when the switch is reset.
`timezone` Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.
`idle` *<idle timeout in minutes Telnet>* Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 5 minutes.
`notice` *<max 1024 char 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).
`cur` Displays the current system parameters.

/cfg/sys/syslog

System Host Log Configuration

```
[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
     console   - Enable/disable console output of syslog messages
     log       - Enable/disable syslogging of features
     cur       - Display current syslog settings
```

Table 6-3 System Configuration Menu Options (/cfg/sys/syslog)

Command Syntax and Usage
host *<new syslog host IP address (such as, 192.4.17.223)>* Sets the IP address of the first syslog host.
host2 *<new syslog host IP address (such as, 192.4.17.223)>* 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 the seven 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 the seven 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.
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.
log *<feature|all> <enable|disable>* Displays a list of features for which syslog messages can be generated. You can choose to enable/disable specific features (such as vlans, gslb, filter), or enable/disable syslog on all available features.
cur Displays the current syslog settings.

/cfg/sys/sshd

SSH Server Configuration Menu

```
[SSHD Menu]
     intrval   - Set Interval for generating the RSA server key
     scpadm    - Set SCP-only admin password
     hkeygen   - Generate the RSA host key
     skeygen   - Generate the RSA server 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 GbE Switch Module, this menu enables Secure Shell access from any SSH client. SSH scripts can be viewed by using the `/cfg/dump` command (see page 274).

NOTE – Except for `cur`, the commands of this menu are only accessible through the management module interface.

Table 6-4 System Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage
`intrval` *<0 - 24>* Set the interval for auto-generation of the RSA server key.
`scpadm` Set the administration password for SCP access.
`hkeygen` Generate the RSA host key.
`skeygen` Generate the RSA server key.
`sshport` *<TCP port number>* Sets the SSH server port number.
`ena` Enables the SCP apply and save.
`dis` Disables the SCP apply and save.
`on` Enables the SSH server.

Table 6-4 System Configuration Menu Options (/cfg/sys/sshd)

Command Syntax and Usage

`off`

Disables the SSH server.

`cur`

Displays the current SSH server configuration.

/cfg/sys/radius

RADIUS Server Configuration

```
[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
     telnet   - Enable or disable RADIUS backdoor for telnet
     on       - Turn RADIUS authentication ON
     off      - Turn RADIUS authentication OFF
     cur      - Display current RADIUS configuration
```

Table 6-5 System 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 configure, default 1645>*

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.

Table 6-5 System Configuration Menu Options (/cfg/sys/radius)

Command Syntax and Usage
`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.
`telnet disable|enable` Enables or disables the RADIUS backdoor for telnet. The `telnet` command also applies to SSH/SCP connections and the Browser-Based Interface (BBI). The default is `disabled`. To obtain the RADIUS backdoor password for your GbESM, contact your IBM Service and Support line.
`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 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 address
     secsrv    - Set secondary TACACS+ server address
     secret    - Set primary TACACS+ server secret
     secret2   - Set secondary TACACS+ server secret
     port      - Set TACACS+ TCP port
     retries   - Set TACACS+ server retries
     timeout   - Set TACACS+ server timeout (seconds)
     telnet    - Enable/disable TACACS+ backdoor for telnet
     cauth     - Enable/disable TACACS+ command authorization
     clog      - Enable/disable TACACS+ command logging
     on        - Turn TACACS+ authentication ON
     off       - Turn TACACS+ authentication OFF
     cur       - Display current TACACS+ configuration
```

Table 6-6 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.
`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 configure, default 49>* 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.
`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.
`telnet disable|enable` Enables or disables the TACACS+ back door for telnet. The `telnet` command also applies to SSH/SCP connections, and the Browser-Based Interface (BBI). The default is `disabled`. To obtain the TACACS+ backdoor password for your GbESM, contact your IBM Service and Support line.

Table 6-6 TACACS+ Server Menu Options (/cfg/sys/tacacs)

Command Syntax and Usage
`cauth disable|enable` Enables or disables TACACS+ command authorization.
`clog disable|enable` Enables or disables TACACS+ command logging.
`on` Enables the TACACS+ server. This is the default setting.
`off` Disables the TACACS+ server.
`cur` Displays current TACACS+ configuration parameters.

/cfg/sys/ntp

NTP Server Configuration

```
[NTP Server Menu]
      prisrv  - Set primary NTP server address
      secsrv  - Set secondary NTP server address
      intrval - Set NTP server resync interval
      tzone   - Set NTP timezone offset from GMT
      dlight  - Enable or disable NTP daylight savings time
      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 6-7 System Configuration Menu Options (/cfg/sys/ntp)

Command Syntax and Usage
`prisrv` *<NTP Server IP address>* Prompts for the IP addresses of the primary NTP server to which you want to synchronize the switch clock.
`secsrv` *<NTP Server IP address>* Prompts for the IP addresses of the secondary NTP server to which you want to synchronize the switch clock.
`intrval` *<resync interval in minutes>* Specifies the interval, that is, how often, in minutes (1-2880), to re-synchronize the switch clock with the NTP server.
`tzone` *<time zone offset, in HH:MM>* Prompts for the NTP time zone offset, in hours and minutes, of the switch you are synchronizing from Greenwich Mean Time (GMT).
`dlight disable|enable` Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled.
`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

```
[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
     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
```

Alteon 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 6-8 System SNMP Menu Options (/cfg/sys/ssnmp)

Command Syntax and Usage
`snmpv3` Displays SNMPv3 menu. To view menu options, see page 164.
`name` *<new string, maximum 64 characters>* Configures the name for the system. The name can have a maximum of 64 characters.
`locn` *<new string, maximum 64 characters>* Configures the name of the system location. The location can have a maximum of 64 characters.
`cont` *<new string, maximum 64 characters>* Configures the name of the system contact. The contact can have a maximum of 64 characters.
`rcomm` *<new SNMP read community string, maximum 32 characters>* Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is *public*.
`wcomm` *<new SNMP write community string, maximum 32 characters>* Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is *private*.
`timeout` Set the timeout value for the SNMP state machine.
`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 RFC2271 to RFC2276.

```
[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 6-9 SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

Command Syntax and Usage

usm *<usmUser number [1-16]>*

This command allows you to create a user security model (USM) entry for an authorized user. You can also configure this entry through SNMP. To view menu options, see page 166.

view *<vacmViewTreeFamily number [1-128]>*

This command allows you to create different MIB views. To view menu options, see page 170.

access *<vacmAccess number [1-32]>*

This command allows you to specify access rights. The View-based Access Control Model defines a set of services that an application can use for checking access rights of the user. You need access control when you have to process retrieval or modification request from an SNMP entity. To view menu options, see page 167.

Table 6-9 SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

`group` *<vacmSecurityToGroup number [1-16]>*

A group maps the user name to the access group names and their access rights needed to access SNMP management objects. A group defines the access rights assigned to all names that belong to a particular group. To view menu options, see page 169.

`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 171.

`taddr` *<snmpTargetAddr number [1-16]>*

This command allows you to configure destination information, consisting of a transport domain and a transport address. This is also termed as transport endpoint. The SNMP MIB provides a mechanism for performing source address validation on incoming requests, and for selecting community strings based on target addresses for outgoing notifications. To view menu options, see page 172.

`tparam` *<target params index [1-16]>*

This command allows you to configure SNMP parameters, consisting of message processing model, security model, security level, and security name information. There may be multiple transport endpoints associated with a particular set of SNMP parameters, or a particular transport endpoint may be associated with several sets of SNMP parameters. To view menu options, see page 173.

`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 174.

`v1v2 disable|enable`

This command allows you to enable or disable the access to SNMP version 1 and version 2. This command is enabled by default.

`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 6-10 User Security Model Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/usm)

Command Syntax and Usage

`name` *<32 character name>*

This command allows you to configure a string up to 32 characters long 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`

This command allows you to configure the authentication protocol between HMAC-MD5-96 or HMAC-SHA-96. The default algorithm is `none`.

`authpw`

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. This command allows you to create or change your password for authentication.

`priv des|none`

This command allows you to configure 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`

This command allows you to create or change the privacy password.

Table 6-10 User Security Model Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/usm)

Command Syntax and Usage
`del` Deletes the USM user entries.
`cur` Displays the USM user entries.

/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 6-11 View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage
`name` *<32 character name>* Defines the name of the group.
`prefix` *<32 character name>* 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.

Table 6-11 View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage
`model usm|snmpv1|snmpv2` Allows you to select the security model to be used.
`level noAuthNoPriv|authNoPriv|authPriv` Defines the minimum level of security required to gain access rights. The level `noAuthNoPriv` means that the SNMP message will be sent without authentication and without using a privacy protocol. The level `authNoPriv` means that the SNMP message will be sent with authentication but without using a privacy protocol. The `authPriv` means that the SNMP message will be sent both with authentication and using a privacy protocol.
`match exact|prefix` If the value is set to `exact`, then all the rows whose contextName exactly matches the prefix are selected. If the value is set to `prefix` then the all the rows where the starting octets of the contextName exactly match the prefix are selected.
`rview` *<32 character view name>* This is a 32 character long 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` *<32 character view name>* This is a 32 character long 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` *<32 character view name>* This is a 32 character 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 6-12 SNMPv3 Group Menu Options (/cfg/sys/ssnmp/snmpv3/group)

Command Syntax and Usage
`model usm|snmpv1|snmpv2` Defines the security model.
`uname` *<32 character name>* Sets the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 166.
`gname` *<32 character name>* The name for the access group as defined in `/cfg/sys/ssnmp/snmpv3/access/name` on page 166.
`del` Deletes the `vacmSecurityToGroup` entry.
`cur` Displays the current `vacmSecurityToGroup` configuration.

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
```

Table 6-13 SNMPv3 View Menu Options (/cfg/sys/ssnmp/snmpv3/view)

Command Syntax and Usage
`name` *<32 character name>* This command defines the name for a family of view subtrees up to a maximum of 32 characters.
`tree` *<object identifier, such as,. 1.3.6.1.2.1.1.1.0, max 32 characters>* This command defines MIB tree, a string of maximum 32 characters, which when combined with the corresponding mask defines a family of view subtrees.
`mask` *<bitmask, max size 32 characters>* This command defines 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/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 6-14 SNMPv3 Community Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/comm)

Command Syntax and Usage
`index` *<32 character name>* Allows you to configure the unique index value of a row in this table consisting of 32 characters maximum.
`name` *<32 character name>* Defines the user name as defined in `/cfg/sys/ssnmp/snmpv3/usm/name` on page 166.
`uname` *<32 character name>* Defines a readable 32 character long string that represents the corresponding value of an SNMP community name in a security model.
`tag` *<list of tag string, max 255 characters>* Allows you to configure a tag of up to 255 characters maximum. This tag 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 6-15 Target Address Table Menu Options (/cfg/sys/ssnmp/snmpv3/taddr)

Command Syntax and Usage

`name` *<32 character name>*
Allows you to configure the locally arbitrary, but unique identifier, target address name associated with this entry.

`addr` *<transport address ip>*
Allows you to configure a transport address IP that can be used in the generation of SNMP traps.

`port` *<transport address port>*
Allows you to configure a transport address port that can be used in the generation of SNMP traps.

`taglist` *<list of tag string, max 255 characters>*
Allows you to configure a list of tags that are used to select target addresses for a particular operation.

`pname` *<32 character name>*
Defines the name as defined in `/cfg/sys/ssnmp/snmpv3/tparam/name` on page 173.

`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 6-16 Target Parameters Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/tparam)

Command Syntax and Usage

`name` *<32 character name>*

Allows you to configure the locally arbitrary, but unique identifier that is associated with this entry.

`mpmodel snmpv1|snmpv2c|snmpv3`

Allows you to configure 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` *<32 character name>*

Defines the name that identifies the user in the USM table (page 166) 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.

Table 6-16 Target Parameters Table Configuration Menu Options (/cfg/sys/ssnmp/snmpv3/tparam)

Command Syntax and Usage

`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 6-17 Notify Table Menu Options (/cfg/sys/ssnmp/snmpv3/notify)

Command Syntax and Usage

`name` *<32 character name>*

Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.

`tag` *<list of tag string, max 255 characters>*

Allows you to configure a tag of 255 characters maximum 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 Menu

```
[System Access Menu]
     mgmt     - Management Network Definition Menu
     user     - User Access Control Menu (passwords)
     http     - Enable/disable HTTP (Web) access
     https    - HTTPS Web Access Menu
     wport    - Set HTTP (Web) server port number
     snmp     - Set SNMP access control
     tnet     - Enable/disable Telnet access
     tnport   - Set Telnet server port number
     cur      - Display current system access configuration
```

Table 6-18 System Configuration Menu Options (/cfg/sys/access)

Command Syntax and Usage
`mgmt` Displays the Management Configuration Menu. To view menu options, see page 176.
`user` Displays the User Access Control Menu. To view menu options, see page 176.
`http disable|enable` Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.
`https disable|enable` Displays the HTTPS Menu. To view menu options, see page 179.
`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).
`snmp disable|read-only|read-write` Disables or provides read-only/write-read SNMP access.
`tnet` Enables or disables telnet access.This command is enabled by default. You will see this command only if you are connected to the switch through the management module.
`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.
`cur` Displays the current system access parameters.

/cfg/sys/access/mgmt

Management Networks Menu

```
[Management Networks Menu]
     add       - Add mgmt network definition
     rem       - Remove mgmt network definition
     cur       - Display current mgmt network definitions
```

This menu is used to define IP address ranges which are allowed to access the switch for management purposes.

Table 6-19 Management Network Menu Options (/cfg/sys/access/mgmt)

Command Syntax and Usage
add *<mgmt network address> <mgmt network mask>* Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the Alteon 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, it will cause the Firewall Load Balancing health checks to fail and will create a “Network Down” state on the network.
rem *<mgmt network address> <mgmt network mask>* Removes a defined network, which consists of a management network address and a management network mask address.
cur Displays the current configuration.

/cfg/sys/access/user

User Access Control Configuration

```
[User Access Control Menu]
     uid       - User ID Menu
     usrpw     - Set user password (user)
     opw       - Set operator password (oper)
     admpw     - Set administrator password (admin)
     cur       - Display current user status
```

NOTE – Passwords can be a maximum of 15 characters.

Table 6-20 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 178.
`usrpw` Sets the user (`user`) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.
`opw` Sets the operator (`oper`) password. The operator password can have a maximum of 15 characters. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports or the entire switch.
`admpw` Sets the administrator (`admin`) password. The super user administrator has complete access to all menus, information, and configuration commands on the GbE Switch Module, including the ability to change both the user and administrator passwords. Access includes "`oper`" functions.
`cur` Displays the current user status.

/cfg/sys/access/user/uid

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 6-21 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. Alteon OS defines these levels as: User, Operator, and Administrator, with User being the most restricted level.
`name` *<8 char max>* Defines the user name of maximum eight characters.
`pswd` *<15 char max>* Sets the user password of up to 15 characters maximum.
`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/https

HTTPS Access Configuration Menu

```
[https Menu]
     https     - Enable/Disable HTTPS Web access
     port      - HTTPS WebServer port number
     generate  - Generate self-signed HTTPS server certificate
     certSave  - save HTTPS certificate
     cur       - Display current SSL Web Access configuration
```

Table 6-22 HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

Command Syntax and Usage

`https`

Enables or disables BBI access (Web access) using HTTPS.

`port` *<TCP port number>*

Defines the HTTPS Web server port number.

`generate`

Allows you to generate a certificate to connect to the SSL to be used during the key exchange. A default certificate is created when HTTPS is enabled for the first time. The user can create a new certificate defining the information that they want to be used in the various fields. For example:

- Country Name (2 letter code) [ ]: CA
- State or Province Name (full name) []: Ontario
- Locality Name (for example, city) []: Ottawa
- Organization Name (for example, company) []: Nortel Networks
- Organizational Unit Name (for example, section) []: Alteon
- Common Name (for example, user's name) []: Mr Smith
- Email (for example, email address) []: info@nortelnetworks.com

You will be asked to confirm if you want to generate the certificate. It will take approximately 30 seconds to generate the certificate. Then the switch will restart SSL agent.

`certSave`

Allows the client, or the Web browser, to accept the certificate and save the certificate to Flash to be used when the switch is rebooted.

`cur`

Displays the current SSL Web Access configuration.

`/cfg/port` *<port alias or number>*
Port Configuration

```
[Port INT1 Menu]
     gig       - Gig Phy Menu
     aclqos    - Acl/Qos Configuration Menu
     8021ppri  - Set default 802.1p priority
     pvid      - Set default port VLAN id
     name      - Set port name
     dscpmrk   - Enable/disable DSCP remarking for port
     tag       - Enable/disable VLAN tagging for port
     fastfwd   - Enable/disable Port Fast Forwarding mode
     ena       - Enable port
     dis       - Disable port
     cur       - Display current port configuration
```

The Port Menu enables you to configure settings for individual switch ports (except MGT1 and MGT2). This command is enabled by default.

Table 6-23 Port Configuration Menu Options (/cfg/port)

Command Syntax and Usage
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 182.
aclqos Displays the ACL Quality of Service Menu. To view menu options, see page 184.
8021ppri *<0-7>* Configures the port’s 802.1p priority level.
pvid *<VLAN number, 1-4095>* 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 *<64 character string>* | **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 is set to None.
dscpmark Enables or disables DSCP re-marking on a port.
tag disable | **enable** Disables or enables VLAN tagging for this port. It is disabled by default.

Table 6-23 Port Configuration Menu Options (/cfg/port)

Command Syntax and Usage
`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.
`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 183.)
`cur` Displays current port parameters.

/cfg/port *<port alias or number>* gig

Port Link Configuration

```
[Gigabit Link Menu]
      speed   - Set link speed
      mode    - Set full or half duplex mode
      fctl    - Set flow control
      auto    - Set auto negotiation
      cur     - Display current gig link configuration
```

Use these menu options to set port parameters for the port link.

NOTE – Since the `speed` and `mode` parameters cannot be set for Gigabit Ethernet ports, these options do not appear on the Gigabit Link Menu.

Link menu options are described in Table 6-24 and appear on the `gig` port configuration menu for the GbE Switch Module. Using this configuration menu, you can set port parameters such as speed, flow control, and negotiation mode for the port link.

Table 6-24 Port Link Configuration Menu Options (/cfg/port/gig)

Command Syntax and Usage
`speed 10|100|any` Sets the link speed. Not all options are valid on all ports. The choices include: ■ "Any," for automatic detection (default) ■ 10 Mbps ■ 100 Mbps ■ 1000 Mbps
`mode full|half|any` Sets the operating mode. The choices include: ■ "Any," for auto negotiation (default) ■ Full-duplex ■ Half-duplex
`fctl rx|tx|both|none` Sets the flow control. The choices include: ■ Receive flow control ■ Transmit flow control ■ Both receive and transmit flow control (default) ■ No flow control

Table 6-24 Port Link Configuration Menu Options (/cfg/port/gig)

Command Syntax and Usage
`auto on|off` Enables or disables auto negotiation for the port.
`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 GbE Switch Module is reset. See the “Operations Menu” on page 277 for other operations-level commands.

/cfg/port *<port alias or number>* aclqos
ACL Port Menu

```
[Port INT1 ACL Menu]
     meter    - ACL Metering Configuration Menu
     re-mark  - ACL Re-mark Configuration Menu
     add      - Add ACL group to this port
     rem      - Remove ACL group from this port
     cur      - Display current ACLs for this port
```

Table 6-25 ACL/QoS Menu Options (/cfg/port/aclqos)

Command Syntax and Usage
`meter` *<meter number, 1-127>* Displays the Metering Menu. To view menu options, see page 185.
`re-mark` *<re-mark number, 1-127>* Displays the Re-Mark Menu. To view menu options, see page 186.
`add` *<ACL number, 1-4096>* Adds the specified ACL Group to the port. You can add multiple ACL Groups to a port, but the total number of precedence levels allowed is eight.
`rem` *<ACL number, 1-4096>* Removes the specified ACL from the port.
`cur` Displays current ACL QoS parameters.

/cfg/port *<port alias or number>* **aclqos/meter** *<meter number>*

ACL Port Metering Menu

```
[Metering Menu]
     cir      - Set committed rate in KiloBits/s
     mbsize   - Set maximum burst size in KiloBits
     enable   - Enable/disable port metering
     dpass    - Set to Drop or Pass out of profile traffic
     assign   - Assign meter to ACL, ACL block or ACL group
     unassign - Unassign meter from ACL, ACL block or ACL group
     reset    - Reset meter parameters
     cur      - Display current settings
```

This menu defines the Access Control profile for the selected ACL group on the port.

Table 6-26 Metering Menu Options (/cfg/port/aclqos/meter)

Command Syntax and Usage
`cir` *<64-1000000>* 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 ACL Metering on the port.
`dpass drop|pass` Configures the ACL Meter to either drop or pass out-of-profile traffic.
`assign acl|blk|grp` *<1-4096>* Adds an ACL, ACL Block, or ACL Group to the ACL Meter on this port.
`unassign acl|blk|grp` *<1-4096>* Removes an ACL, ACL Block, or ACL Group from the ACL Meter on this port.
`reset` Reset ACL Metering parameters to their default values.
`cur` Displays current ACL Metering parameters.

/cfg/port *<port alias or number>* aclqos/re-mark *<re-mark number>*

Re-Mark Menu

```
[Re-mark Menu Menu]
     inprof    - In Profile Menu
     outprof   - Out Profile Menu
     assign    - Assign re-mark action to ACL item
     unassign  - Unassign re-mark action from ACL item
     reset     - Reset re-mark settings
     cur       - Display current settings
```

You can choose to re-mark IP header data for the selected ACL Group on the port. 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 6-27 Re-Mark Options (/cfg/port/aclqos/re-mark)

Command Syntax and Usage
`inprof` Displays the Re-Mark In-Profile Menu. To view menu options, see page 187.
`outprof` Displays the Re-Mark Out-of-Profile Menu. To view menu options, see page 189.
`assign acl|blk|grp` *<1-4096>* Assign an ACL, ACL Block, or ACL Group for DSCP remarking on this port.
`unassign acl|blk|grp` *<1-4096>* Remove an ACL, ACL Block, or ACL Group from DSCP remarking on this port.
`reset` Reset ACL Re-Mark parameters to their default values.
`cur` Displays current Re-Mark parameters.

/cfg/port *<port alias or number>* aclqos/re-mark *<ACL group number>*/inprof

Re-Marking In-Profile 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 6-28 Re-Mark Options (/cfg/port/aclqos/re-mark/inprof)

Command Syntax and Usage
up1p Displays the Re-Mark In-Profile Update User Priority Menu. To view menu options, see page 188.
updscp *<0-63>* Sets 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 In-Profile parameters.

/cfg/port *<port alias or number>* **aclqos/re-mark/inprof** *<ACL group number>***/up1p**

Update User Priority Menu

```
[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 6-29 User Priority Options (/cfg/port/aclqos/re-mark/inprof/up1p)

Command Syntax and Usage
`value` *<0-7>* Defines 802.1p value. The value is the priority bits information in the packet structure.
`utosp enable|disable` Enable or disable mapping of TOS (Type of Service) priority to 802.1p priority for In-Profile packets. When enabled, the TOS value is used to set the 802.1p value.
`reset` Resets UP1P settings to their default values.
`cur` Displays current Re-Mark In-Profile User Priority parameters.

/cfg/port *<port alias or number>* **aclqos/ re-mark** *<ACL group number>***/outprof**

Re-Marking Out-of-Profile Menu

```
[Re-marking - Out Of Profile Menu]
     updscp    - Set the update DSCP
     reset     - reset update DSCP setting
     cur       - Display current settings
```

Table 6-30 Out-of-Profile Options (/cfg/port/aclqos/re-mark/outprof)

Command Syntax and Usage
updscp *<0-63>* Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value. The switch sets the DSCP value on Out-of-Profile packets.
reset Resets the update DSCP parameters for Out-of-Profile packets to their default values.
cur Displays current Re-Mark Out-of-Profile parameters.

/cfg/l2

Layer 2 Menu

```
[Layer 2 Menu]
     8021x     - 802.1x Menu
     mrst      - Multiple Spanning Tree/Rapid Spanning Tree Menu
     stp       - Spanning Tree Menu
     trunk     - Trunk Group Menu
     thash     - IP Trunk Hash Menu
     lacp      - Link Aggregation Control Protocol Menu
     vlan      - VLAN Menu
     upfast    - Enable/disable Uplink Fast
     update    - UplinkFast station update rate
     cur       - Display current layer 2 parameters
```

Table 6-31 Configuration Menu Options (/cfg/l2)

Command Syntax and Usage
`8021x` Displays the 802.1x Configuration Menu. To view menu options, see page 191.
`mrst` Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu. To view menu options, see page 196.
`stg` *<group number [1-16]>* Displays the Spanning Tree Configuration Menu. To view menu options, see page 202.
`trunk` *<trunk group number (1-2)>* Displays the Trunk Group Configuration Menu. To view menu options, see page 207.
`thash` Displays the IP Trunk Hash Menu. To view menu options, see page 208.
`lacp` Displays the Link Aggregation Control Protocol Menu. To view menu options, see page 210.
`vlan` *<VLAN number (1-4095)>* Displays the VLAN Configuration Menu. To view menu options, see page 211.
`upfast enable|disable` Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover. **Note**: When enabled, this feature increases bridge priorities to 65500 for all STGs and path cost by 3000 for all external STP ports.
`update` *<VLAN number (10-200)>* Configures the station update rate. The default value is 40.
`cur` Displays current Layer 2 parameters.

/cfg/l2/8021x
802.1x Configuration

```
[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 6-32 Spanning Tree Configuration Menu (/cfg/l2/8021x)

Command Syntax and Usage
`global` Displays the global 802.1x Configuration Menu. To view menu options, see page 203.
`port` *<port alias or number>* Displays the 802.1x Port Menu. To view menu options, see page 205.
`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]
     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
     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 6-33 Spanning Tree Configuration Menu (/cfg/l2/8021x/global)

Command Syntax and Usage
`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 from the authentication server. The default value is 30 seconds.

Table 6-33 Spanning Tree Configuration Menu (/cfg/l2/8021x/global)

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`.
`default` Resets the global 802.1x parameters to their default values.
`cur` Displays current global 802.1x parameters.

`/cfg/l2/8021x/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
    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 6-34 Spanning Tree Configuration Menu (/cfg/l2/8021x/port)

Command Syntax and Usage

`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 from the authentication server. The default value is 30 seconds.

Table 6-34 Spanning Tree Configuration Menu (/cfg/l2/8021x/port)

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`.
`default` Resets the 802.1x port parameters to their default values.
`global` Applies current global 802.1x configuration parameters to the port.
`cur` Displays current 802.1x port parameters.

/cfg/l2/mrst
Rapid Spanning Tree Protocol/Multiple Spanning Tree Protocol Configuration

```
[Multiple Spanning Tree Menu]
      cist    - Common and Internal Spanning Tree menu
      name    - Set MST region name
      version - Set Version of this MST region
      maxhop  - Set Maximum Hop Count for MST (4 - 60)
      mode    - Spanning Tree Mode
      on      - Globally turn Multiple Spanning Tree (MSTP/RSTP) ON
      off     - Globally turn Multiple Spanning Tree (MSTP/RSTP) OFF
      cur     - Display current MST parameters
```

Alteon OS supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

There are 16 spanning tree groups that can be configured on the switch. MRST is turned off by default.

NOTE – When Multiple Spanning Tree is turned on, VLAN 4095 is moved from Spanning Tree Group 16 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, VLAN 4095 is moved back to Spanning Tree Group 16.

Table 6-35 Multiple Spanning Tree 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 198.
`name` *<32 character string>* Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.
`version` *<1-65535>* Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within a MSTP region must have the same version number.

Table 6-35 Multiple Spanning Tree Configuration Menu Options (/cfg/l2/mrst)

Command Syntax and Usage
`maxhop` *<4-60>* Configures the maximum number of bridge hops a packet may to traverse before it is dropped. The range is from 4 to 60 hops. The default is 20.
`mode rstp`|**`mstp`** Selects either Rapid Spanning Tree mode (`rstp`) or Multiple Spanning Tree mode (`mstp`). The default mode is RSTP.
`on` Globally turns RSTP/MSTP ON. **Note**: When RSTP is turned on, the configuration parameters for STP group 1 apply to RSTP.
`off` Globally turns RSTP/MSTP OFF.
`cur` Displays the current RSTP/MSTP configuration.

/cfg/l2/mrst/cist
Common Internal Spanning Tree Configuration

```
[Common Internal Spanning Tree Menu]
  brg     - CIST Bridge parameter menu
  port    - CIST Port parameter menu
  default - Default Common Internal Spanning Tree and Member parameters
  cur     - Display current CIST parameters
```

Table 6-36 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 6-36 Common Internal Spanning Tree Menu Options (/cfg/l2/mrst/cist)

Command Syntax and Usage
`brg` Displays the CIST Bridge Menu. To view menu options, see page 199.
`port` *<port number>* Displays the CIST Port Menu. To view menu options, see page 200.
`default` Resets all CIST parameters to their default values.
`cur` Displays the current CIST configuration.

/cfg/l2/mrst/cist/brg
CIST Bridge Configuration

```
[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 or RSTP mode. CIST parameters do not affect operation of STP/PVST.

Table 6-37 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, and the default is 32768.
`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 number>* CIST Port Configuration

```
[CIST Port 1 Menu]
    prior    - Set port Priority (0-240)
    cost     - Set port Path Cost (1-200000000)
    hello    - Set CIST port Hello Time (1-10 secs)
    link     - Set MSTP link type (auto, p2p, or shared; default: auto)
    edge     - Enable/disable edge port
    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. For each port, RSTP/MSTP is turned on by default.

Table 6-38 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` *<1-200000000>* Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 20000 for Gigabit ports.
`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.
`link` *<auto, p2p, or shared; default: auto>* Defines the type of link connected to the port, as follows: **`auto`**: Configures the port to detect the link type, and automatically match its settings. **`p2p`**: Configures the port for Point-To-Point protocol. **`shared`**: Configures the port to connect to a shared medium (usually a hub). The default link type is **`auto`**.

Table 6-38 CIST Port Configuration Menu Options (/cfg/l2/mrst/cist/port)

Command Syntax and Usage
`edge disable|enable` 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). This command is disabled by default.
`on` Enables MRST on the port.
`off` Disables MRST on the port.
`cur` Displays the current CIST port configuration.

/cfg/l2/stg

Spanning Tree Configuration

```
[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
```

Alteon OS supports the IEEE 802.1d Spanning Tree Protocol (STP). STG is used to prevent loops in the network topology. There are 16 spanning tree groups that can be configured on the switch (STG 16 is reserved for management). This command is turned on by default.

NOTE – When VRRP is used for active/active redundancy, STG must be enabled.

Table 6-39 Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage
brg Displays the Bridge Spanning Tree Menu. To view menu options, see page 203.
port *<port alias or number>* Displays the Spanning Tree Port Menu. To view menu options, see page 205.
add *<VLAN number (1-4095)>* Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter.
remove *<VLAN number (1-4095)>* Breaks the association between a VLAN and a spanning tree and requires an external VLAN ID as a parameter.
clear Removes all VLANs from a spanning tree.
on Globally enables Spanning Tree Protocol.
off Globally disables Spanning Tree Protocol.

Table 6-39 Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage
`default` Restores a spanning tree instance to its default configuration.
`cur` Displays current Spanning Tree Protocol parameters.

/cfg/l2/stg/brg

Bridge Spanning Tree Configuration

```
[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)
      aging   - Set bridge Aging Time (1-65535 secs, 0 to disable)
      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
- Bridge aging time

Table 6-40 Bridge Spanning Tree Menu Options (/cfg/l2/stg/brg)

Command Syntax and Usage
`prior` *<new bridge priority (0-65535)>* Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. **RSTP/MSTP**: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768.
`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 198).
`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 198).
`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 198).
`aging` *<new bridge Aging Time (1-65535 secs, 0 to disable)>* Configures the forwarding database aging time. The aging time specifies the amount of time the bridge waits without receiving a packet from a station before removing the station from the forwarding database. The range is 1 to 65535 seconds, and the default is 300 seconds. To disable aging, set this parameter to 0.
`current` Displays the current bridge STG parameters.

When configuring STG bridge parameters, the following formulas must be used:

- $2*(fwd-1) \geq mxage$
- $2*(hello+1) \leq mxage$

/cfg/l2/stg *<STP Group Index>*/port *<port alias or number>*

Spanning Tree Port Configuration

```
[Spanning Tree Port EXT1 Menu]
  prior     - Set port Priority (0-255)
  cost      - Set port Path Cost
  link     - Set port link type (auto, p2p, or shared; default: auto)
  edge      - Enable/disable edge port
  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

The **`port`** option of STG is turned on by default.

Table 6-41 Spanning Tree Port Menu (/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 range is 0 to 255, and the default is 128. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.
`cost` *<new port Path 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. Generally speaking, the faster the port, the lower the path cost. The range is 1 to 65535. The default is 10 for 100Mbps ports, and 1 for Gigabit ports. A value of 0 indicates that the default cost will be computed for an auto negotiated link speed.
`link` *`<auto, p2p, or shared; default: auto>`* 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).

Table 6-41 Spanning Tree Port Menu (/cfg/l2/stg/port)

Command Syntax and Usage
`edge disable|enable` 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).
`on` Enables STG on the port.
`off` Disables STG on the port.
`cur` Displays the current STG port parameters.

/cfg/l2/trunk *<trunk group number>*

Trunk Configuration

```
[Trunk group 1 Menu]
     add     - Add port to trunk group
     rem     - Remove port from trunk group
     failovr - Enable/disable failover support
     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 GbE Switch Modules 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 three trunk groups can be configured on the GbE Switch Module, with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to four ports/trunks can belong to the same trunk group.
- Best performance is achieved when all ports in a trunk are configured for the same speed.
- Trunking from non-Alteon devices must comply with Cisco® EtherChannel® technology.

By default, the trunk group is empty and disabled.

Table 6-42 Trunk Configuration Menu Options (/cfg/l2/trunk)

Command Syntax and Usage
`add` *<port alias or number (EXT1-EXT6)>* Adds a physical port to the current trunk group.
`rem` *<port alias or number (EXT1-EXT6)>* Removes a physical port from the current trunk group.
`failovr` Sets trunk group failover to enabled or disabled.
`ena` Enables the current trunk group.
`dis` Turns the current trunk group off.
`del` Removes the current trunk group configuration.
`cur` Displays current trunk group parameters.

/cfg/l2/thash

IP Trunk Hash menu

```
[IP Trunk Hash Menu]
     set       - IP Trunk Hash Settings Menu
     cur       - Display current IP trunk hash configuration
```

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

Table 6-43 IP Trunk Hash commands (/cfg/l2/thash)

Command Syntax and Usage
`set` Displays the Trunk Hash Settings menu. To view menu options, see page 208.
`cur` Display current trunk hash configuration.

/cfg/l2/thash/set

Layer 2 IP Trunk Hash menu

```
[l2 IP 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
```

Trunk hash parameters are set globally for the GbE Switch Module. You can enable one or two 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 layer 2 IP trunk hash parameters for the GbESM.

Table 6-44 Layer 2 IP Trunk Hash commands (/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 layer 2 trunk hash setting.

/cfg/l2/lacp

Link Aggregation Control Protocol menu

```
[LACP Menu]
     sysprio   - Set LACP system priority
     timeout   - Set LACP system timeout scale for timing out partner
                 info
     port      - LACP port Menu
     cur       - Display current LACP configuration
```

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

Table 6-45 Link Aggregation Control Protocol (/cfg/l2/lacp)

Command Syntax and Usage
`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**: Nortel Networks recommends 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.
`port` *<port alias or number>* Displays the LACP Port menu. To view menu options, see page 210.
`cur` Display current LACP configuration.

/cfg/l2/lacp/port *<port alias or number>*

LACP Port menu

```
[LACP Port EXT1 Menu]
     mode      - Set LACP mode
     prio      - Set LACP port priority
     adminkey  - Set LACP port admin key
     cur       - Display current LACP port configuration
```

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

Table 6-46 Link Aggregation Control Protocol (/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. Default is 128.
`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.
`cur` Displays the current LACP configuration for this port.

`/cfg/l2/vlan` *<VLAN number>*

VLAN Configuration

```
[VLAN 1 Menu]
      name     - Set VLAN name
      stg      - Assign VLAN to a Spanning Tree Group
      add      - Add port to VLAN
      rem      - Remove port from VLAN
      def      - Define VLAN as list of ports
      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 the VLAN, delete the VLAN, and change the port membership of the VLAN. For more information on configuring VLANs, see "Setup Part 3: VLANs" on page 31.

By default, the VLAN menu option is disabled except VLAN 1, which is enabled all the time. Internal server ports (INTx) and external ports (EXT1-EXT6) are in VLAN 1 by default.

Table 6-47 VLAN Configuration Menu Options (/cfg/l2/vlan)

Command Syntax and Usage
`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 [1-16]>* Assigns a VLAN to a Spanning Tree Group.
`add` *<port alias or number>* Adds port(s) or trunk group(s) to the VLAN membership.
`rem` *<port alias or number>* Removes port(s) or trunk group(s) from this VLAN.
`def` *<list of port numbers>* Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, internal server ports (INTx) and external ports (EXT1-EXT6) are in VLAN 1.
`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 180).

/cfg/l3
Layer 3 Menu

```
[Layer 3 Menu]
     if       - Interface Menu
     gw       - Default Gateway Menu
     route    - Static 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
     igmp     - IGMP Menu
     dns      - Domain Name System Menu
     bootp    - Bootstrap Protocol Relay Menu
     vrrp     - Virtual Router Redundancy Protocol Menu
     rtrid    - Set router ID
     cur      - Display current IP configuration
```

Table 6-48 Configuration Menu Options (/cfg/l3)

Command Syntax and Usage
`if` *<interface number (1-128)>* Displays the IP Interface Menu. To view menu options, see page 214.
`gw` *<default gateway number (1-132)>* Displays the IP Default Gateway Menu. To view menu options, see page 215.
`route` Displays the IP Static Route Menu. To view menu options, see page 217.
`arp` Displays the Address Resolution Protocol Menu. To view menu options, see page 217.
`frwd` Displays the IP Forwarding Menu. To view menu options, see page 219.
`nwf` *<Network filter number [1-256]>* Displays the Network Filter Configuration Menu. To view menu options see page 219.
`rmap` *<route map number [1-32]>* Displays the Route Map Menu. To view menu options see page 221.
`rip` Displays the Routing Interface Protocol Menu. To view menu options, see page 226.

Table 6-48 Configuration Menu Options (/cfg/l3)

Command Syntax and Usage
`ospf` Displays the OSPF Menu. To view menu options, see page 228.
`bgp` Displays the Border Gateway Protocol Menu. To view menu options, see page 237.
`igmp` Displays the IGMP Menu. To view menu options, see page 243.
`dns` Displays the IP Domain Name System Menu. To view menu options, see page 249.
`bootp` Displays the Bootstrap Protocol Menu. To view menu options, see page 250.
`vrrp` Displays the Virtual Router Redundancy Configuration Menu. To view menu options, see page 251.
`rtrid` *<<IP address (such as, 192.4.17.101)>* Sets the router ID.
`cur` Displays the current IP configuration.

/cfg/l3/if *<interface number>*

IP Interface Configuration

```
[IP Interface 1 Menu]
      addr     - Set IP address
      mask     - Set subnet mask
      vlan     - Set VLAN number
      relay    - Enable or disable BOOTP relay
      ena      - Enable interface
      dis      - Disable interface
      del      - Delete interface
      cur      - Display current interface configuration
```

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

NOTE – To maintain connectivity between the management module and the GbE Switch Module, use the management module interface to change the IP address of the switch.

Table 6-49 IP Interface Menu Options (/cfg/l3/if)

Command Syntax and Usage
`addr` *<IP address (such as 192.4.17.101)>* Configures the IP address of the switch interface using dotted decimal notation.
`mask` *<IP subnet mask (such as 255.255.255.0)>* Configures the IP subnet address mask for the interface using dotted decimal notation.
`vlan` *<VLAN number (1-4095)>* Configures the VLAN number for this interface. Each interface can belong to one VLAN, though any VLAN can have multiple IP interfaces in it.
`relay disable|enable` Enables or disables the BOOTP relay on this interface. It is enabled by default.
`ena` Enables this IP interface.
`dis` Disables this IP interface.
`del` Removes this IP interface.
`cur` Displays the current interface settings.

`/cfg/l3/gw` *<gateway number>*

Default Gateway Configuration

```
[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
      vlan     - Set VLAN number
      ena      - Enable default gateway
      dis      - Disable default gateway
      del      - Delete default gateway
      cur      - Display current default gateway configuration
```

NOTE – The switch can be configured with up to 132 gateways. Gateways one to four are reserved for default gateways. Gateway 132 is reserved for the management VLAN.

This option is disabled by default.

Table 6-50 Default Gateway 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 1 to 120 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. This command is disabled by default.
`vlan` *<VLAN number (1-4095)>* Sets the VLAN to be assigned to this default IP gateway.
`ena` Enables the gateway for use.
`dis` Disables the gateway.
`del` Deletes the gateway from the configuration.
`cur` Displays the current gateway settings.

Default Gateway Metrics

For information about configuring which gateway is selected when multiple default gateways are enabled, see page 216.

/cfg/l3/route

IP Static Route Configuration

```
[IP Static Route Menu]
      add      - Add static route
      rem      - Remove static route
      cur      - Display current static routes
```

Up to 128 static routes can be configured.

Table 6-51 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.
`rem` *<destination> <mask>* Removes a static route. The destination address of the route to remove must be specified using dotted decimal notation.
`cur` Displays the current IP static 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 6-52 ARP Configuration Menu Options (/cfg/l3/arp)

Command Syntax and Usage
`static` Displays Static ARP menu. To view options, see page 218.
`rearp` *<2-120 minutes>* Defines re-ARP period in minutes. You can set this duration between two and 120 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 learnt 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
     cur      - Display current static ARP configuration
```

Table 6-53 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.
`cur` Displays current static ARP configuration.

/cfg/l3/frwd

IP Forwarding Configuration

```
[IP Forwarding Menu]
      dirbr    - Enable or disable forwarding directed broadcasts
      on       - Globally turn IP Forwarding ON
      off      - Globally turn IP Forwarding OFF
      cur      - Display current IP Forwarding configuration
```

Table 6-54 IP Forwarding Configuration Menu Options (/cfg/l3/frwd)

Command Syntax and Usage
dirbr disable|enable Enables or disables forwarding directed broadcasts. This command is disabled by default.
on Enables IP forwarding (routing) on the GbE Switch Module.
off Disables IP forwarding (routing) on the GbE Switch Module. Forwarding is turned off by default.
cur Displays the current IP forwarding settings.

/cfg/l3/nwf

Network Filter Configuration

```
[IP Network Filter 1 Menu]
      addr     - IP Address
      mask     - IP Subnet mask
      enable   - Enable Network Filter
      disable  - Disable Network Filter
      delete   - Delete Network Filter
      cur      - Display current Network Filter configuration
```

Table 6-55 IP Network Filter Menu Options (/cfg/l3/nwf)

Command Syntax and Usage
`addr` *<IP address, such as 192.4.17.44>* Sets the starting IP address for this filter. The default address is 0.0.0.0.
`mask` *<subnet mask, such as 255.255.255.0>* Sets the IP subnet mask that is used with `/cfg/l3/nwf/addr` to define the range of IP addresses that will be accepted by the peer when the filter is enabled. 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

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 6-56 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 223.
aspath *<number 1-8>* Displays the Autonomous System (AS) Filter menu. For more information, see page 224.
ap *<AS number> [<AS number>] [<AS number>]* | **none** Sets the AS path preference of the matched route. One to three path preferences can be configured.
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 *<(0-4294967294)>* | **none** Sets the metric of the matched route.

Table 6-56 Routing Map Menu Options (/cfg/l3/rmap) (Continued)

Command Syntax and Usage
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 2 routes have more cost than Type 2. ■ none—Removes the OSPF metric.
prec *<value (1-256)>* Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.
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 6-57 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" on page 219 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

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 6-58 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.
`current` Displays the current Autonomous System filter configuration.

/cfg/l3/rip

Routing Information Protocol Configuration

```
[Routing Information Protocol Menu]
     if        - RIP Interface Menu
     update    - Set update period in seconds
     on        - Globally turn RIP ON
     off       - Globally turn RIP OFF
     current   - Display current RIP configuration
```

The RIP Menu is used for configuring Routing Information Protocol parameters. This option is turned off by default.

Table 6-59 Routing Information Protocol Menu (/cfg/l3/rip)

Command Syntax and Usage
`if` *<1-128>* Displays the RIP Interface menu. For more information, see page 226.
`update` *<1-120>* Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.
`on` Globally turns RIP ON.
`off` Globally turns RIP OFF.
`cur` Displays the current RIP configuration.

/cfg/l3/rip/if *<interface number>*

Routing Information Protocol Interface Configuration

```
[RIP Interface 1 Menu]
     version   - Set RIP version
     supply    - Enable/disable supplying route updates
     listen    - Enable/disable listening to route updates
     default   - Set default route action
     poison    - Enable/disable poisoned reverse
     trigg     - Enable/disable triggered updates
     mcast     - Enable/disable multicast updates
     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 Menu is used for configuring Routing Information Protocol parameters. This option is turned off by default.

NOTE – Do not configure RIP1 parameters if your routing equipment uses RIP version 2.

Table 6-60 Routing Information Protocol Menu (/cfg/l3/rip/if)

Command Syntax and Usage
`version` Configures the RIP version used by this interface. The default value is version `1`.
`supply disable|enable` This command is disabled by default. When enabled, the switch supplies routes to other routers.
`listen disable|enable` This command is disabled by default. When enabled, the switch learns routes from other routers.
`default disable|enable` 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. This command is disabled by default.
`poison disable|enable` This command is disabled by default. When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon.

Table 6-60 Routing Information Protocol Menu (/cfg/l3/rip/if)

Command Syntax and Usage
`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 `disabled`.
`mcast disable|enable` Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is `disabled`.
`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` Configures the authentication key password.
`enable` Enables this RIP interface.
`disable` Disables this RIP interface.
`current` Displays the current RIP configuration.

/cfg/l3/ospf

Open Shortest Path First Configuration

```
[Open Shortest Path First Menu]
      aindex   - OSPF Area (index) menu
      range    - OSPF Summary Range menu
      if       - OSPF 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 6-61 OSPF Configuration Menu Options (/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 229 to view menu options.

`range` *<range number (1-16)>*

Displays summary routes menu for up to 16 IP addresses. See page 231 to view menu options.

`if` *<interface number (1-128)>*

Displays the OSPF interface configuration menu. See page 232 to view menu options.

`virt` *<virtual link (1-3)>*

Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See page 233 to view menu options.

`md5key` *<key ID [1-255>*

Assigns a string to MD5 authentication key. See

`host` *<host entry number (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 235 to view menu options.

`redist` *<fixed|static|rip|ebgp|ibgp>*

Displays Route Distribution Menu See page 236 to view menu options.

Table 6-61 OSPF Configuration Menu Options (/cfg/l3/ospf)

Command Syntax and Usage
lsdb *<LSDB limit (0-2000, 0 for no limit)>* Sets the link state database limit.
default *<metric [1-16777215]> <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 GbE Switch Module.
off Disables OSPF on the GbE Switch Module.
cur Displays the current OSPF configuration settings.

/cfg/l3/ospf/aindex

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 6-62 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.
`spf` *<interval [0-255]>* Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.
`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

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 6-63 OSPF Summary Range Configuration Menu Options (/cfg/l3/ospf/range)

Command Syntax and Usage
`addr` *<IP Address (such as, 192.4.17.101)>* Displays the base IP address for the range.
`mask` *<IP address (such as, 192.4.17.101>* Displays the IP address mask for the range.
`aindex` *<area index [0-2]>* Displays the area index used by the GbE Switch Module.
`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.
`current` Displays the current OSPF summary range.

/cfg/l3/ospf/if

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
      dead    - Set dead interval in seconds
      trans   - Set transit delay in seconds
      retra   - Set retransmit interval in seconds
      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 6-64 OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)

Command Syntax and Usage
`aindex` *<area index [0-2]>* Displays the OSPF area index.
`prio` *<priority value (0-127)>* Displays the assigned priority value to the GbE Switch Module's OSPF interfaces. (A priority value of 127 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` *<cost value (1-65535)>* Displays 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` *<value [1-65535]>* Displays the interval in seconds between the `hello` packets for the intefaces.
`dead` *<value [1-65535]>* Displays the health parameters of a `hello` packet, which is set for an interval of seconds before declaring a silent router to be down.
`trans` *<value [0-3600]>* Displays the transit delay in seconds.
`retra` *<value [0-3600]>* Displays the retransmit interval in seconds.

Table 6-64 OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)

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.
`enable` Enables OSPF interface.
`disable` Disables OSPF interface.
`delete` Deletes OSPF interface.
`cur` Displays the current settings for OSPF interface.

/cfg/l3/ospf/virt

OSPF Virtual Link Configuration Menu

```
[OSPF 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
     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 6-65 OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt)

Command Syntax and Usage
`aindex` *<area index [0-2]>* Displays the OSPF area index.
`hello` *<value [1-65535]>* Displays the authentication parameters of a hello packet, which is set to be in an interval of seconds.
`dead` *<value [1-65535]>* Displays the health parameters of a hello packet, which is set to be in an interval of seconds. Default is 40 seconds.
`trans` *<value [1-3600]>* Displays the delay in transit in seconds. Default is one seconds.
`retra` *<value [1-3600]>* Displays the retransmit interval in seconds. Default is five seconds.
`nbr` *<NBR router ID (IP address)>* Displays the router ID of the virtual neighbor. Default is 0.0.0.0.
`key` *<password>* Displays the password (up to eight characters) for each virtual link. Default is `none`.
`mdkey` *<key ID [1-256]>* | **`none`** Sets MD5 key ID for each virtual link. Default is `none`.
`enable` Enables OSPF virtual link.
`disable` Disables OSPF virtual link.
`delete` Deletes OSPF virtual link.
`cur` Displays the current OSPF virtual link settings.

/cfg/l3/ospf/host

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 6-66 OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)

Command Syntax and Usage
`addr` *<IP address (such as, 192.4.17.101)>* Displays the base IP address for the host entry.
`aindex` *<area index [0-2]>* Displays the area index of the host.
`cost` *<cost value [1-65535]>* Displays 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 6-67 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 [1-16777215]><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

OSPF MD5 Key Configuration Menu

```
[OSPF MD5 Key 1 Menu]
     key      - Set authentication key
     delete   - Delete key
     cur      - Display current MD5 key configuration
```

Table 6-68 OSPF MD5 Key Configuration Menu Options (/cfg/ip/ospf/md5key)

Command Syntax and Usage
`key` 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

```
[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.

The BGP Menu enables 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 Alteon OS implementation, the GbE Switch Module does not advertise BGP routes that are learned from other BGP "speakers".

The BGP menu option is turned off by default.

NOTE – Fixed routes are subnet routes. There is one fixed route per IP interface.

Table 6-69 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 239.
`aggr` *<aggregate number (1-16)>* Displays the Aggregation Menu. To view menu options, see page 242.
`as` *<1 - 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
      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
      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 6-70 BGP Peer Configuration Options (/cfg/l3/bgp/peer)

Command Syntax and Usage
`redist` Displays BGP Redistribution Menu. To view the menu options, see page 241.
`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.
`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. It is set at 90 seconds by default.
`alive` *<keepalive time (0, 1-21845)>* Sets the keep-alive time for the specified peer in seconds. It is set at 0 by default.

Table 6-70 BGP Peer Configuration Options (/cfg/l3/bgp/peer)

Command Syntax and Usage
`advert` *<min adv time (1-65535)>* Sets time in seconds between advertisements.
`retry` *<connect retry interval (1-65535)>* Sets connection retry interval in seconds.
`orig` *<min orig time (1-65535)>* Sets the minimum time between route originations in 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.
`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.
`ena` Enables this peer configuration.
`dis` Disables this peer configuration.
`del` Deletes this peer configuration.
`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
      vip     - Enable/disable advertising VIP routes
      cur     - Display current redistribution configuration
```

Table 6-71 BGP Redistribution Configuration 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.

Defaults routes can be configured as import, originate, redistribute, or none.

None: No routes are configured

Import: Import these routes.

Originate: The switch sends a default route to peers even though 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.

Table 6-71 BGP Redistribution Configuration Menu Options (/cfg/l3/bgp/peer/redist)

Command Syntax and Usage
`vip disable|enable` Enables or disables advertising VIP routes.
`current` Displays current redistribution configuration.

`/cfg/l3/bgp/aggr` *(aggregation number)*

BGP Aggregation Configuration

```
[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 filters that specify the routes/range of IP destinations a peer router will accept from other peers. A route must match a filter to be installed in the routing table. By default, the first filter is enabled and the rest of the filters are disabled.

Table 6-72 BGP Filter Configuration Options (/cfg/l3/bgp/aggr)

Command Syntax and Usage
`addr` *<IP address (such as 192.4.17.101)>* Defines the starting IP address for this filter, 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 filter is enabled. The default address is 0.0.0.0.
`ena` Enables this BGP filter.
`dis` Disables this BGP filter.

Table 6-72 BGP Filter Configuration Options (/cfg/l3/bgp/aggr)

Command Syntax and Usage
`del` Deletes this BGP filter.
`cur` Displays the current BGP filter configuration.

/cfg/l3/igmp
IGMP Configuration

```
[IGMP Menu]
       snoop    - IGMP Snoop Menu
       mrouter  - Static Multicast Router Menu
       igmpflt  - IGMP Filtering Menu
```

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 6-73 IGMP Snoop Menu (/cfg/l3/igmp)

Command Syntax and Usage
`snoop` Displays the IGMP Snoop Menu. To view menu options, see page 244.
`mrouter` Displays the Static Multicast Router Menu. To view menu options, see page 245.
`igmpflt` Displays the IGMP Filtering Menu. To view menu options, see page 246.

/cfg/l3/igmp/snoop

IGMP Snooping Configuration

```
[IGMP Snoop Menu]
      timeout  - Set report timeout
      mrto     - Set multicast router timeout
      robust   - Set expected packet loss on subnet
      fastlv   - Enable/disable Fastleave processing in VLAN
      ena      - Enable IGMP Snooping
      dis      - Disable IGMP Snooping
      cur      - Display current IGMP Snooping configuration
```

Table 6-74 describes the commands used to configure IGMP Snooping.

Table 6-74 IGMP Snoop Menu (/cfg/l3/igmp/snoop)

Command Syntax and Usage
`timeout` *<1-255 seconds>* 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.
`mrto` *<1-255 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 255 seconds. The default is 60 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.
`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.
`ena` Enables IGMP Snooping.
`dis` Disables IGMP Snooping.
`cur` Displays the current IGMP Snooping parameters.

/cfg/l3/igmp/mrouter

IGMP Static Multicast Router Configuration

```
[Static Multicast Router Menu]
       add     - Add port as Multicast Router Port
       rem     - Remove port as Multicast Router Port
       cur     - Display current Multicast Router configuration
```

Table 6-75 describes the commands used to configure a static multicast router.

NOTE – When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

Table 6-75 IGMP Static Multicast Router Menu (/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 or 2) of the multicast router. **Note**: Port number must be an external port (EXT1-EXT6).
`remove` *<port number>* *`<VLAN number>`* *`<IGMP version number>`* Removes a static multicast router from the selected port/VLAN combination.
`cur` Displays the current IGMP Static Multicast Router parameters.

/cfg/l3/igmp/igmpflt

IGMP Filtering Configuration

```
[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 6-76 describes the commands used to configure an IGMP filter.

Table 6-76 IGMP Filtering Menu (/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 247.
`port` *<port number>* Displays the IGMP Filtering Port Menu. To view menu options, see page 248.
`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

```
[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 6-77 describes the commands used to define an IGMP filter.

Table 6-77 IGMP Filter Definition Menu (/cfg/l3/igmp/igmpflt/filter)

Command Syntax and Usage
`range` *<IP multicast address (such as 224.0.0.10)> <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.
`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

```
[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 6-78 describes the commands used to configure a port for IGMP filtering.

Table 6-78 IGMP Filter Definition Menu (/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/dns

Domain Name System Configuration

```
[Domain Name System Menu]
      prima    - Set IP address of primary DNS server
      secon    - Set IP address of secondary DNS server
      dname    - Set default domain name
      cur      - Display current DNS configuration
```

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

Table 6-79 Domain Name Service Menu Options (/cfg/l3/dns)

Command Syntax and Usage
`prima` *<IP address (such as 192.4.17.101)>* You will be prompted to set the IP address for your primary DNS server. Use dotted decimal notation.
`secon` *<IP address (such as 192.4.17.101)>* You will be prompted to set the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.
`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

```
[Bootstrap Protocol Relay Menu]
      addr     - Set IP address of BOOTP server
      addr2    - Set IP address of second BOOTP server
      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 GbE Switch Module.

BOOTP relay menu is turned off by default.

Table 6-80 Bootstrap Protocol Relay Configuration Menu Options (/cfg/l3/bootp)

Command Syntax and Usage
`addr` *<IP address (such as, 192.4.17.101>* Sets the IP address of the BOOTP server.
`addr2` *<IP address (such as, 192.4.17.101>>* Sets the IP address of the second BOOTP server.
`on` Globally turns on BOOTP relay.
`off` Globally turns off BOOTP relay.
`cur` Displays the current BOOTP relay configuration.

/cfg/l3/vrrp
VRRP Configuration

```
[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
      trnkfo   - Enable/disable trunk failover
      on       - Globally turn VRRP ON
      off      - Globally turn VRRP OFF
      cur      - Display current VRRP configuration
```

Virtual Router Redundancy Protocol (VRRP) support on GbE Switch Modules 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. Alteon 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 *Alteon OS 21.0 Application Guide*.

Table 6-81 Virtual Router Redundancy Protocol 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 up to 128 virtual routers on this switch. To view menu options, see page 252.
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 Alteon switches in a hot-standby failover configuration where only one switch is active at any given time. To view menu options, see page 256.
if *<interface number (1-128)>* Displays the VRRP Virtual Router Interface Menu. To view menu options, see page 259.

Table 6-81 Virtual Router Redundancy Protocol Options (/cfg/l3/vrrp)

Command Syntax and Usage
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 260.
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.
trnkfo disable|enable When enabled, allows L2 Trunk Failover to be enabled when VRRP is enabled (but not hot standby processing). By default, this option is disabled.
on Globally enables VRRP on this switch.
off Globally disables VRRP on this switch.
cur Displays the current VRRP parameters.

/cfg/l3/vrrp/vr *<router number>*

Virtual Router Configuration

```
[VRRP Virtual Router 1 Menu]
      track   - Priority Tracking Menu
      vrid    - Set virtual router ID
      addr    - Set IP address
      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
```

This menu is used for configuring up to 128 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 6-82 VRRP Virtual Router Options (/cfg/l3/vrrp/vr)

Command Syntax and Usage

`track`

Displays the VRRP Priority Tracking Menu for this virtual router. Tracking is an Alteon OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 255.

`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.

`if` *<interface number (1-128)>*

Selects a switch IP interface (between 1 and 128). 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 value is 1.

`prio` *<priority (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.

Table 6-82 VRRP Virtual Router Options (/cfg/l3/vrrp/vr)

Command Syntax and Usage
`adver` *<seconds (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

```
[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 260).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option (see `preem` in Table 6-82 on page 253) 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 6-83 VRRP 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

```
[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 GbE Switch Module 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 GbE Switch Modules in a hot-standby failover configuration, where only one switch is active at any time.

Table 6-84 VRRP Virtual Router Group Options (/cfg/l3/vrrp/group)

Command Syntax and Usage
`track` Displays the VRRP Priority Tracking Menu for the virtual router group. Tracking is an Alteon OS proprietary extension to VRRP, used for modifying the standard priority system used for electing the master router. To view menu options, see page 257.
`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 (1-128)>* Selects a switch IP interface (between 1 and 128). The default switch IP interface number is 1.

Table 6-84 VRRP Virtual Router Group Options (/cfg/l3/vrrp/group)

Command Syntax and Usage

`prio` *<priority (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. 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` *<seconds (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

```
[Virtual Router Group 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 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 6-85 Virtual Router Group Priority Tracking Options (/cfg/l3/vr/group/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/if *<interface number>*
VRRP Interface Configuration

NOTE – The *interface-number* (1 to 128) 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 6-86 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

```
[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 255), the priority level for the virtual router is increased by an amount defined through this menu.

Table 6-87 VRRP Tracking Options (/cfg/l3/vrrp/track)

Command Syntax and Usage
`vrs` *<0-254>* Defines the priority increment value (1 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 (1 through 254) for active IP interfaces detected on this switch. The default value is 2.
`ports` *<0-254>* Defines the priority increment value (1 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 255) are enabled.

/cfg/qos
Quality of Service Menu

```
[QOS Menu]
     8021p     - 802.1p Menu
     dscp      - Dscp Menu
```

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

Table 6-88 Quality of Service options (/cfg/qos)

Command Syntax and Usage
8021p Displays 802.1p configuration menu. To view menu options, see page 261.
dscp Displays DSCP configuration menu. To view menu options, see page 263.

/cfg/qos/8021p
802.1p Menu

```
[802.1p Menu]
     priq      - Set priority to COS queue mapping
     qweight   - Set weight to a COS queue
     cur       - Display current 802.1p configuration
```

This feature provides the GbESM 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 6-89 802.1p menu options (/cfg/qos/8021p)

Command Syntax and Usage
`priq` *<0-7> <0-7>* Maps the 802.1p priority of to the Class of Service queue (COSq) priority. Enter the 802.1p priority value (0-7), followed by the Class of Service queue (0-7) that handles the matching traffic.
`qweight` *<0-7> <0-15>* Configures the weight of the selected Class of Service queue (COSq). Enter the queue number (0-7), followed by the scheduling weight (0-15).
`cur` Displays the current 802.1p parameters.

/cfg/qos/dscp

DSCP 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 6-90 DSCP menu options (/cfg/qos/dscp)

Command Syntax and Usage
dscp *<0-63> <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 (0-8)>* 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 Menu

```
[ACL Menu]
     acl       - Access Control List Item Config Menu
     block     - Access Control List Block Config Menu
     group     - Access Control List Group Config Menu
     cur       - Display current ACL configuration
```

Use the this menu to create Access Control Lists, ACL Blocks, and ACL Groups. ACLs define matching criteria used for IP filtering and Quality of Service functions.

Table 6-91 ACL menu options (/cfg/acl)

Command Syntax and Usage
`acl` *<1-4096>* Displays Access Control List configuration menu. To view menu options, see page 265.
`block` *<1-4096>* Displays ACL Block configuration menu. To view menu options, see page 270.
`group` *<1-4096>* Displays ACL Group configuration menu. To view menu options, see page 271.
`cur` Displays the current ACL parameters.

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

Access Control List Menu

```
[ACL 1 Menu]
     ethernet - Ethernet Header Options Menu
     ipv4     - IP Header Options Menu
     tcpudp   - TCP/UDP Header Options Menu
     pktfmt   - Set to filter specific packet format types
     egrport  - Set to filter for packets egressing this port
     action   - Set filter action
     stats    - Enable/disable statistics for this acl
     reset    - Reset filtering parameters
     cur      - Display current filter configuration
```

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

Table 6-92 ACL menu options (/cfg/acl/acl x)

Command Syntax and Usage
ethernet Displays the ACL Ethernet configuration menu. To view menu options, see page 266.
ipv4 Displays the ACL IP version 4 configuration menu. To view menu options, see page 267.
tcpudp Displays the ACL TCP/UDP configuration menu. To view menu options, see page 268.
pktfmt *<packet format>* Displays the ACL Packet Format configuration menu. To view menu options, see page 269.
egrport *<port alias or number>* Configures the ACL to function on egress packets.
action permit|deny|setcos Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the Class of Service queue that handles the packets.
stats e|d Enables or disables the statistics collection for the Access Control List.
reset Resets the ACL parameters to their default values.
cur Displays the current ACL parameters.

/cfg/acl/acl *<ACL number>*/ethernet

Ethernet Filtering 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 6-93 Ethernet Filtering options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage
`smac` *<MAC address (such as 00:60:cf:40:56:00)>* Defines the source MAC address for this ACL.
`dmac` *<MAC address (such as 00:60:cf:40:56:00)>* Defines the destination MAC address for this ACL.
`vlan` *<1-4095> <VLAN mask (0xfff)>* Defines a VLAN number and mask for this ACL.
`etype ARP`|**`IP`**|**`IPv6`**|**`MPLS`**|**`RARP`**|**`any`**|**`0xXXXX`** 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

IP version 4 Filtering 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 IPv4 matching criteria for an ACL.

Table 6-94 IP version 4 Filtering options (/cfg/acl/acl x/ipv4)

Command Syntax and Usage

sip *<IP address>*

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>*

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 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 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 6-95 TCP/UDP Filtering options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage

`sport` *<1-65535>*

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` *<1-65535>*

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)>*

Defines a TCP/UDP flag for the ACL.

Table 6-95 TCP/UDP Filtering options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage
`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>*/pktfmt

Packet Format Filtering 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 6-96 Packet Format Filtering options (/cfg/acl/acl x/pktfmt)

Command Syntax and Usage
`ethfmt eth2|SNAP|LLC` Defines the Ethernet format for the ACL.
`tagfmt 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/block *<ACL Block number>*

ACL Block Menu

```
[ACL Block 1 Menu]
     addacl    - Add ACL item to block
     remacl    - Remove ACL item from block
     cur       - Display current ACL items in block
```

This menu allows you to compile one or more ACLs into an ACL Block. Each ACL in the ACL Block must fall within the same mask.

Table 6-97 ACL Block options (/cfg/acl/block x)

Command Syntax and Usage
addacl *<1-4096>* Adds the selected ACL to the ACL Block.
remacl *<1-4096>* Removes the selected ACL from the ACL Block.
cur Displays the current ACL block parameters.

/cfg/acl/group *<ACL Group number>*

ACL Group Menu

```
[ACL Group 1 Menu]
     add       - Add ACL or ACL block to group
     rem       - Remove ACL or ACL block from group
     cur       - Display current ACL items in group
```

This menu allows you to compile one or more ACLs and ACL Blocks into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

Table 6-98 ACL Group options (/cfg/acl/group x)

Command Syntax and Usage
add acl|blk *<1-4096>* Adds the selected ACL or ACL Block to the ACL Group.
rem acl|blk *<1-4096>* Removes the selected ACL or ACL Block from the ACL Group.
cur Displays the current ACL group parameters.

/cfg/pmirr

Port Mirroring Menu

```
[Port Mirroring Menu]
      mirror   - Enable/Disable Mirroring
      monport  - Monitoring Port based PM Menu
      cur      - Display All Mirrored and Monitoring Ports
```

Port mirroring is disabled by default. For more information about port mirroring on the GbE Switch Module, see "Appendix A: Troubleshooting" in the *Alteon 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 monitored 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 6-99 Port Mirroring menu options (/cfg/pmirr)

Command Syntax and Usage
`mirror disable|enable` Enables or disables port mirroring
`monport` *<port alias or number>* Displays port-mirroring menu. To view menu options, see page 272.
`cur` Displays current settings of the mirrored and monitoring ports.

/cfg/pmirr/monport

Port-Mirroring Menu

```
[Port EXT1 Menu]
     add       - Add "Mirrored" port and VLANs
     rem       - Rem "Mirrored" port and VLANs
     delete    - Delete this "Monitor" port
     cur       - Display current Port Mirroring configuration
```

Table 6-100 Port-Based Port-Mirroring 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 mirrored 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/setup
Setup

The setup program steps you through configuring the system date and time, BOOTP, IP, Spanning Tree, port speed/mode, VLAN parameters, and IP interfaces.

To start the setup program, at the Configuration# prompt, enter:

```
Configuration# setup
```

For a complete description of how to use setup, see Chapter 2, “First-Time 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 275.

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

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

Where *server* is the TFTP server IP address or hostname, and *filename* is the name of the target script configuration file.

NOTE – The output file is formatted with line-breaks but no carriage returns—the file cannot be viewed with editors that require carriage returns (such as Microsoft Notepad).

NOTE – If the 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 *<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 <TFTP server> <filename>
```

Where *server* is the TFTP server IP 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
     passwd   - Change current user password
     clrlog   - Clear syslog messages
     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 7-1 Operations Menu Options (/oper)

Command Syntax and Usage
port *<port alias or number>* Displays the Operational Port Menu. To view menu options, see page 279.
vrrp Displays the Operational Virtual Router Redundancy Menu. To view menu options, see page 280.
ip Displays the IP Operations Menu, which has one sub-menu/option, the Operational Border Gateway Protocol Menu. To view menu options, see page 280.

Table 7-1 Operations Menu Options (/oper)

Command Syntax and Usage
`passwd` *<15 char max>* Allows the user to change the password. You need to enter the current password in use for validation.
`clrlog` Clears all Syslog messages.
`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

```
[Operations Port INT1 Menu]
     8021x    - 8021.x Menu
     ena      - Enable port
     dis      - Disable port
     cur      - Current port state
```

Operations-level port options are used for temporarily disabling or enabling a port, and for changing Remote Monitoring (RMON) status on a port.

Table 7-2 Operations-Level Port Menu Options (/oper/port)

Command Syntax and Usage
`8021x` Displays the 802.1x Port Menu. To view menu options, see page 280.
`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.
`cur` Displays the current settings for the port.

/oper/port *<port alias or number>*/8021x
Operations-Level Port 802.1x Options

```
[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 7-3 Operations-Level Port 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.

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

Table 7-4 Virtual Router Redundancy Operations 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

```
[IP Operations Menu]
     bgp     - Operational Border Gateway Protocol Menu
```

Table 7-5 IP Operations Menu Options (/oper/ip)

Command Syntax and Usage

`bgp`

Displays the Border Gateway Protocol Operations Menu. To view the menu options see page 282.

/oper/ip/bgp

Operations-Level BGP Options

```
[Border Gateway Protocol Operations Menu]
      start   - Start peer session
      stop    - Stop peer session
      current - Current BGP operational state
```

Table 7-6 IP Operations Menu Options (/oper/ip)

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.

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 TFTP

In addition to the Boot Menu, you can use SNMP to work with switch image and configuration files. Refer to "Working with Switch Images and Configuration Files" on page 318.

/boot
Boot Menu

```
[Boot Options Menu]
       sched - Scheduled Switch Reset Menu
       image - Select software image to use on next boot
       conf  - Select config block to use on next boot
       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.

Scheduled Reboot of the Switch

This feature allows the switch administrator to schedule a reboot to occur at a particular time in 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 with the help of the following sub-menu:

/boot/sched

Scheduled Reboot Menu

```
[Boot Schedule Menu]
     set       - Set switch reset time
     cancel    - Cancel pending switch reset
     cur       - Display current switch reset schedule
```

Updating the Switch Software Image

The switch software image is the executable code running on the GbE Switch Module. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software available for your GbE Switch Module, go to:

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

Click on software updates. Use `/boot/cur` to determine the current software version.

Upgrading the software image on your switch requires the following:

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

Downloading 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 download new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

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

To download a new software to your switch, you will need the following:

- The image or boot software loaded on a TFTP server on your network
- The hostname or IP address of the 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" on page 249.

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

1. **At the `Boot Options#` prompt, enter:**

```
Boot Options# gtimg
```

2. **Enter the name of the switch software to be replaced:**

```
Enter name of switch software image to be replaced
 ["image1"/"image2"/"boot"]: <image>
```

3. **Enter the hostname or IP address of the TFTP server.**

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

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

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

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

5. **The system prompts you to confirm your request.**

You should next select a software image to run, as described below.

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 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> <hostname or server-IP-addr> <server-file-
name>
```

3. **Enter the name or the IP address of the TFTP server:**

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

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

```
Enter name of file on 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 20.0.1.0
Upload will transfer image2 (1889411 bytes) to file "test"
 on TFTP server 192.1.1.1.
Confirm upload operation [y/n]: y
```

Selecting a Configuration Block

When you make configuration changes to the GbE Switch Module, 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 GbE Switch Module was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured GbE Switch Module is moved to a network environment where it will be re configured for a different purpose.

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.

NOTE – Resetting the switch causes the date and time to revert to default values. Use `/cfg/sys/date` and `/cfg/sys/time` to reenter the current date and time.

To reset the switch, at the `Boot Options#` prompt, enter:

```
>> Boot Options# reset
```

You are prompted to confirm your request.

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
     arp       - ARP Cache Manipulation Menu
     route     - IP Route Manipulation Menu
     igmp      - IGMP Multicast Group Menu
     uudmp     - Uuencode FLASH dump
     ptdmp     - Upload FLASH dump via FTP/TFTP
     cldmp     - Clear FLASH dump
     panic     - Dump state information to FLASH and reboot
     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 GbE Switch Module after any one of the following occurs:

- The switch administrator forces a switch *panic*. The `panic` option, found in the Maintenance Menu, causes the switch to dump state information to flash memory, and then causes the switch to reboot.
- 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 9-1 Maintenance Menu Options (/maint)

Command Syntax and Usage
`sys` Displays the System Maintenance Menu. To view menu options, see page 293.
`fdb` Displays the Forwarding Database Manipulation Menu. To view menu options, see page 293.
`debug` Displays the Debugging Menu. To view menu options, see page 295.
`arp` Displays the ARP Cache Manipulation Menu. To view menu options, see page 295.
`route` Displays the IP Route Manipulation Menu. To view menu options, see page 296.
`igmp` Displays the IGMP Maintenance Menu. To view menu options, see page 298.
`uudmp` Displays dump information in uuencoded format. For details, see page 298.
`ptdmp hostname, filename [-mgmt|-data]` Saves the system dump information via TFTP. For details, see page 299.
`cldmp` Clears dump information from flash memory. For details, see page 299.
`panic` Dumps MP information to FLASH and reboots. For details, see page 300.
`tsdmp` Dumps all GbE Switch Module 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 Options

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
```

Table 9-2 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 Tech support group.

/maint/fdb
Forwarding Database Options

```
[FDB Manipulation Menu]
      find     - Show a single FDB entry by MAC address
      port     - Show FDB entries for a single port
      vlan     - Show FDB entries for a single VLAN
      dump     - Show all FDB entries
      del      - Delete an FDB entry
      clear    - Clear entire FDB
```

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

Table 9-3 FDB Manipulation Menu Options (/maint/fdb)

Command Syntax and Usage
`find` *<MAC address>* [*<VLAN>*] Displays a single database entry by its MAC address. You are prompted to enter the MAC address of the device. Enter the MAC address using the `xx:xx:xx:xx:xx:xx` format (such as `08:00:20:12:34:56`) or `xxxxxxxxxxxx` format (such as `080020123456`).
`port` *<port alias or number>* Displays all FDB entries for a particular port.
`vlan` *<VLAN number (1-4095)>* Displays all FDB entries on a single VLAN.
`dump` Displays all entries in the Forwarding Database. For details, see page 64.
`del` *<MAC address> [<VLAN>]* Removes a single FDB entry.
`clear` Clears the entire Forwarding Database from switch memory.

/maint/debug
Debugging Options

```
[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 IBM Service Support.

Table 9-4 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 25, 2001; 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/arp
ARP Cache Options

```
[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 9-5 Address Resolution Protocol 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 85.

/maint/route
IP Route Manipulation

```
[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 9-6 IP Route Manipulation Menu Options (/maint/route)

<table>
<tr><th>Command Syntax and Usage</th></tr>
<tr><td><b>find</b> <i>&lt;IP address (such as, 192.4.17.101)&gt;</i>
Shows a single route by destination IP address.</td></tr>
<tr><td><b>gw</b> <i>&lt;default gateway address (such as, 192.4.17.44)&gt;</i>
Shows routes to a default gateway.</td></tr>
<tr><td><b>type indirect|direct|local|broadcast|martian|multicast</b>
Shows routes of a single type. For a description of IP routing types, see Table 4-23 on page 84</td></tr>
<tr><td><b>tag fixed|static|addr|rip|ospf|bgp|broadcast|martian|vip</b>
Shows routes of a single tag. For a description of IP routing tags, see Table 4-24 on page 85</td></tr>
<tr><td><b>if</b> <i>&lt;interface number (1-128)&gt;</i>
Shows routes on a single interface.</td></tr>
<tr><td><b>dump</b>
Shows all routes.</td></tr>
<tr><td><b>clear</b>
Clears the route table from switch memory.</td></tr>
</table>

NOTE – To display all routes, you can also refer to “IP Routing Information” on page 83.

/maint/igmp
IGMP Group Information

```
[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
     dump     - Show all groups
     clear    - Clear group table
```

Table 9-7 describes the IGMP Snooping Maintenance commands.

Table 9-7 IGMP Multicast Group Menu Options (/maint/igmp)

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.
`dump` Displays information for all multicast groups.
`clear` Clears the IGMP group table.

/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 299.

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` *<server> <filename>*
TFTP System Dump Put

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

NOTE – If the 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 TFTP, at the `Maintenance#` prompt, enter:

```
Maintenance# ptdmp <server> <filename>
```

Where *server* is the TFTP server IP 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.
```

/maint/panic
Panic Command

The panic command causes the switch to immediately dump state information to flash memory and automatically reboot.

To select panic, at the Maintenance# prompt, enter:

```
>> Maintenance# panic
A FLASH dump already exists.
Confirm replacing existing dump and reboot [y/n]:
```

Enter **y** to confirm the command:

```
Confirm dump and reboot [y/n]: y
```

The following messages are displayed:

```
Starting system dump...done.

Rebooted because of PANIC command.
Booting complete  0:01:01 Thu Jul  1, 2003:
Version 1.0.0.18 from FLASH image1, active config block.

No POST errors (0xff).

Production Mode.
```

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 October 30, 2002. 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
Alteon OS Syslog Messages

The following syntax is used when outputting syslog messages:

<Time stamp><Log Label>`Web OS`*<Thread ID>*`:`*<Message>*

where

- *<Timestamp>*

  The time of the message event is displayed in month day hour:minute:second format. For example: `Aug 19 14:20:30`

- *<Log Label>*

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

- *<Thread ID>*

  This is the software thread that reports the log message. The following thread IDs are recorded: `stg`, `ip`, `console`, `telnet`, `vrrp`, `system`, `web server`, `ssh`, and `bgp`

- *<Message>*: The log message

Following is a list of potential syslog messages. To keep this list as short as possible, only *<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_WARNING

FILTER "filter *<filter number>* fired on port *<port number>*, *<source IP address>* -> *<destination IP address>*, [*<ICMP type>*], [*<IP protocol>*], [*<layer-4 ports>*], [*<TCP flags>*]"

LOG_ALERT

STP	Own BPDU received from port <port_id>
STP	STG <stg>, topology change detected
STP	CIST topology change detected
STP	STG <stg>, new root bridge
STP	CIST new root bridge
IP	Cannot contact default gateway <ip_address>
VRRP	Received errored advertisement from <ip_address>
VRRP	Received incorrect password from <ip_address>
VRRP	Received incorrect addresses from <ip_address>
VRRP	Received incorrect advertisement interval <seconds> from <ip_address>
VRRP	Synchronization from non-configured peer <ip_address>
VRRP	Synchronization from non-configured peer <ip_address> was blocked
BGP	Notification (<reason>) received from <BGP peer ip_address>
BGP	Session with <BGP peer ip_address> failed (<reason>)
SFP	Inserted at port EXT<num> is UNAPPROVED! Port is DISABLED.
SFP	Removed at port EXT<num>
SFP	Inserted at port EXT<num>

LOG_CRITICAL

SSH	Can’t allocate memory in load_MP_INT
SSH	Currently not enough resource for loading RSA private key
SSH	Currently not enough resource for loading RSA public key
SYSTEM	Temperature exceeds threshold
SFP	Failed to Read SFP ID for port EXT<num>
SFP	Failed to Select SFP for port EXT<num> ID
SFP	Voltage (<volt>) is UNDER Range on port EXT<num>. Port is DISABLED
SFP	Voltage (<volt>) is OVER Range on port EXT<num>
SFP	Failed to Read SFP Voltage|Temperature for port EXT<num>
SFP	Failed to Select SFP for port EXT<num> voltage|temperature.
SFP	Temperature (<temp>) is UNDER|OVER Range on port EXT<num>
SFP	Poll SFP Failed to get SFP Status
SFP	Inserted at port EXT<num> has I2C FAILURE! Port is DISABLED.
SFP	TX Fault on port EXT<num>. Port is DISABLED.

LOG_ERROR

MGMT	`PANIC at <file>:<line> in thread <thread id>`
MGMT	VERIFY at <file>:<line> in thread <thread id>
MGMT	ASSERT at <file>:<line> in thread <thread id>
NTP	Cannot contact <primary|secondary> NTP server <ip_address>
NTP	Unable to listen to NTP port
STP	Error: Error writing STG config to FLASH
STP	Error: Error writing config to FLASH
MGMT	Apply not done
MGMT	Save not done
MGMT	<apply|save|diff> is issued by another user. Try later.
CLI	Error: Error writing %s config to FLASH

LOG_ERROR (continued)

CLI	New Path Cost for Port <port_id> is invalid
CLI	PVID <vlan_id> for port <port_id> is not created
CLI	RADIUS secret must be 1-32 characters long
CLI	Please configure primary RADIUS server address
CLI	STP changes can’t be applied since STP is OFF
CLI	Trunk group <trunk_id> contains ports with different PVIDs
CLI	Trunk group <trunk_id> has more than <max_trunk_ports> ports
CLI	Trunk group <trunk_id> contains no ports but is enabled
CLI	Not all ports in trunk group <trunk_id> are in VLAN <vlan_id>
CLI	Trunk groups <trunk_id> and <trunk_id> can not share the same port

LOG_ERROR (continued)

PORT_MIRR	Port Mirroring changes are not applied
CLI	Broadcast address for IP interface <interface_id> is invalid
CLI	IP Interfaces <interface_id> and <interface_id> are on the same subnet
MGMT	Unapplied changes reverted
MGMT	Unsaved changes reverted
CLI	SNMP source trap interface <IF> is not enabled
CLI	Password already taken
CLI	Radius is already turned ON
CLI	Cannot ena/dis primary admin user
CLI	Cannot change primary admin COS

LOG_ERROR (continued)

CLI	Cannot change primary admin username
CLI	Cannot delete primary admin
CLI	Error: Enabled user <user> has no username
CLI	Error: Enabled user <user> has no password
CLI	New combination of Bridge Timers for STG <group> is invalid
CLI	Need maxage <= 2*(frwd-1) and maxage >= 2*(hello+1)
CLI	Multiple VLAN members in non default STG <group>
CLI	Duplicate VLAN members in STGs <gr1> and <gr2>
CLI	VRRP hot-standby port (<port>) is part of a STG (<group>) with STP turned on
CLI	Error writing active config to FLASH! - Another save is in progress -OR- - Configuration is too large -OR- - Unknown error

LOG_ERROR (continued)

CLI	A previous apply is being executed. Try later.
CLI	RADIUS secret must be 1-<len> characters long
CLI	Please configure primary RADIUS server address.
CLI	TACACS+ secret must be 1-<len> characters long
CLI	Please configure primary TACACS+ server address.
CLI	Port Mirroring changes are not applied
VRRP	cfg_sync_tx_putsn: ABORTED
VRRP	Synchronization RX connection RESET.
VRRP	Synchronization RX connection TIMEOUT.
VRRP	Synchronization RX connection UNKNOWN CLOSE.

LOG_ERROR (continued)

VRRP	Synchronization RX connection UNREACHABLE.
VRRP	Synchronization TX Error.
VRRP	Synchronization TX connection RESET.
VRRP	Synchronization TX connection TIMEOUT.
VRRP	Synchronization TX connection UNREACHABLE.
VRRP	Synchronization TX connection UNKNOWN CLOSE.
VRRP	Synchronization connection RCLOSE by peer.
VRRP	Synchronization connection Wait-For-Close Timeout.
VRRP	Synchronization connection Transmit Timeout.
VRRP	Synchronization Receive Timeout

LOG_ERROR(continued)

VRRP	Synchronization Receive UNKNOWN Timeout
VRRP	Sync receive in progress ... cannot start Sync
VRRP	Sync already in progress ... cannot start Sync
VRRP	Config Sync route find error.
VRRP	Config Sync tcp_open error.
VRRP	Config Synchronization Timeout - Resuming Console thread
VRRP	New configuration did not validate (rc=<code>)
VRRP	New configuration did not apply (rc=<code>)
VRRP	Sync config apply error.
VRRP	Attempting to redirect a previously redirected input

LOG_ERROR (continued)

VRRP	Sync rx tcp open Error
VRRP	Sync Version/Password Failed-No Version/Password Line
VRRP	Sync Version Failed - peer:<host> config:<version>
VRRP	Sync Password Failed-Bad Password
VRRP	Sync of switches of different hardware types is not supported
VRRP	Synchronization connection RCLOSE before RX.
VRRP	Sync transmit already in progress ... cannot start Sync
VRRP	Sync receive in progress ... cannot start Sync
VRRP	Sync receive already in progress ... cannot start Sync receive
VRRP	Sync transmit in progress ... cannot start Sync receive

LOG_ERROR (continued)

VRRP	Multiple static routes have same destination
VRRP	Virtual router <vr_id> must have sharing disabled when hotstandby is enabled
VRRP	Virtual router group must be enabled when hotstandby is enabled
VRRP	At least one virtual router must be enabled when group is enabled
VRRP	Virtual router group must have sharing disabled when hotstandby is enabled
VRRP	Virtual router group must have preemption enabled when hotstandby is enabled
VRRP	Virtual router <vr_id> must have an IP address
VRRP	Virtual router <vr_id> cannot have same VRID and VLAN as <vlan_id>
VRRP	Virtual router <vr_id> cannot have same IP address as <ip_address>
VRRP	Virtual router <vr_id> corresponding virtual server <server_id> is not enabled

LOG_ERROR (continued)

CLI	Duplicate default entry
CLI	BGP peer <bgp_peer_id> must have an IP address
CLI	BGP peers <bgp_peer_id> and <bgp_peer_id> have same address
CLI	BGP peer <bgp_peer_id> have same address as IP interface <ip_interface_id>
CLI	BGP peer <bgp_peer_id> IP interface <ip_interface_id> is not enabled

LOG_NOTICE

SYSTEM	Rebooted <last_reset_information>
SYSTEM	Rebooted <last_reset_information> administrator logged in
SYSTEM	Enable auto negotiation for copper GIG port: <port>
SYSTEM	Change fiber GIG port <port> mode to full duplex
SYSTEM	Change fiber GIG port <port> speed to 1000
MGMT	Boot config block changed
MGMT	Boot image changed
MGMT	Switch reset from CLI
MGMT	Syslog host changed to <ip_address>
MGMT	Syslog host changed to this host

LOG_NOTICE (continued)

MGMT	Second syslog host changed to <ip_address>
MGMT	Second syslog host changed to this host
MGMT	Next boot will use active config block
MGMT	User password changed
MGMT	Operator password changed
MGMT	Administrator password changed
MGMT	RADIUS server timeouts
MGMT	Failed login attempt via TELNET from host %s
MGMT	Failed login attempt via the CONSOLE
MGMT	PASSWORD FIX-UP MODE IN USE

LOG_NOTICE (continued)

MGMT	<login_level> login on Console
MGMT	" <login_level> <""idle timeout""|""logout""> from Console"
MGMT	" <login_level> <""connection closed""|""idle timeout""|""logout""> from"
MGMT	Administrator logout from BBI
MGMT	<login_level> login from host <ip_address>
MGMT	System clock set to <time>
MGMT	PANIC command from CLI
MGMT	Switch reset scheduled at <time>
MGMT	Switch reset at <time> has been cancelled
MGMT	Scheduled switch reboot

LOG_NOTICE (continued)

MGMT	<mins> minute%s until scheduled reboot
MGMT	Password for <user> changed by <user>, notifying admin to save.
MGMT	Temperature OK
VLAN	Default VLAN can not be deleted
IP	" default gateway <ip_address> <""enabled""|""disabled"">"
IP	Default gateway <ip_address> operational
SSH	scp <login_level> login
SSH	" scp <login_level> <""connection closed""|""idle timeout""|""logout"">"
PORT_MIRR	Port mirroring is enabled
PORT_MIRR	Port mirroring is disabled

LOG_NOTICE (continued)

SYSTEM	Management Port enabled/disabled state can only be controlled by Management Module.
SYSTEM	Management Port can only be enabled/disabled by the Management Module
SYSTEM	Cannot change the Management IP Interface VLAN
SYSTEM	Cannot enable/disable the Management IP Interface
SYSTEM	Cannot enable/disable forwarding on Management IP Interface
SYSTEM	Cannot delete the Management IP Interface
SYSTEM	Management VLAN can not be disabled
SYSTEM	Default VLAN can not be deleted
SYSTEM	Management VLAN can not be deleted
SYSTEM	Management Port enabled/disabled state can only be controlled by Management Module.

LOG_NOTICE (continued)

SYSTEM	Management Port can only be enabled/disabled by the Management Module
SYSTEM	Cannot change the Management IP Interface VLAN
SYSTEM	Cannot enable/disable the Management IP Interface
SYSTEM	Cannot enable/disable forwarding on Management IP Interface
SYSTEM	Cannot delete the Management IP Interface
SYSTEM	Management VLAN can not be disabled
SYSTEM	Default VLAN can not be deleted
SYSTEM	Management VLAN can not be deleted
SYSTEM	Rebooted <cause and time of reboot>
SYSTEM	Management Port cannot be configured as a Monitor Port.
VRRP	Virtual router <ip_address> is now master
VRRP	Virtual router <ip_address> is now backup
BGP	Session established with <BGP_peer_ip_address>

LOG_INFO

MGMT	New configuration applied
MGMT	New configuration saved
MGMT	Unsaved changes reverted
MGMT	Could not revert unsaved changes
MGMT	" <image1|image2> downloaded from host <ip_address>, file <file_name> <software_version>"
MGMT	Serial EEPROM downloaded from host <ip_address> file <file_name>
MGMT	<login_level> login on Console
MGMT	" <login_level> <""idle timeout""|""logout""> from Console"
MGMT	<login_level> login from host <ip_address>
MGMT	" <login_level> <""connection closed""|""idle timeout""|""logout""> from Telnet/SSH."

LOG_INFO (continued)

MGMT	Unsupported GBIC refused
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error. Trying again
MGMT	Flash Write Error. Failed to allocate buffer. Quitting
MGMT	Flash Write Error
MGMT	FLASH ERROR - invalid address used
SSH	scp <login_level> login
SSH	" scp <login_level> <""connection closed""|""idle timeout""|""logout"">"
SSH	Server key autogen starts
SSH	Server key autogen completes

LOG_INFO (continued)

SSH	Server key autogen timer timeouts
VRRP	Synchronizing to <host> ...
VRRP	Config Synchronization Transmit Successful.
VRRP	New configuration validated
VRRP	New configuration applied
VRRP	New configuration did not save (rc=<code>)
VRRP	New configuration saved
VRRP	Restoring Current Config.
VRRP	Synchronizing from <host> ...
VRRP	Config Synchronization Receive Successful.
VRRP	Synchronization connection early RCLOSE in RX.

APPENDIX B
Alteon OS SNMP Agent

The Alteon OS SNMP agent supports SNMP Version 1. 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). Alteon WebSystems is registered as Vendor 1872. Detailed SNMP MIBs and trap definitions of the Alteon OS SNMP agent can be found in the following Alteon OS enterprise MIB documents:

- `altroot.mib`
- `aosswitch.mib`
- `aosphysical.mib`
- `aosnetwork.mib`
- `aosacl`
- `aosqos`
- dot1x.mib
- `zoetrap.mib`

Users may specify up to two trap hosts for receiving SNMP Traps. The agent will send the SNMP Trap to the specified hosts when appropriate. Traps are not sent if there is no host specified.

Alteon OS SNMP agent supports the following standard MIBs:

- RFC 1213 - MIB II (System, Interface, Address Translation, IP, ICMP, TCP, UDP, SNMP Groups)
- RFC 1573 - MIB II Extension (IFX table)
- RFC 1643 - EtherLike MIB
- RFC 1493 - Bridge MIB
- RFC 1757 - RMON MIB (Statistics, History, Alarm, Event Groups)
- RFC 1850 for OSPF
- RFC 1657 for BGP
- RFC 2037

Alteon 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 Alteon OS:

Table 9-8 Alteon OS-Supported Enterprise SNMP Traps

Trap Name	Description
altSwPrimaryPowerSupplyFailure	Signifies that the primary power supply failed.
altSwFanFailure	Signifies that the fan has failed.
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	The newMaster trap indicates that the sending agent has transitioned to 'Master' state.
altSwVrrpNewBackup	The newBackup trap indicates that the sending agent has transitioned to 'Backup' state.
altSwVrrpAuthFailure	A vrrpAuthFailure trap 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	A altSwLoginFailure trap signifies that someone failed to enter a valid username/password combination.

Table 9-8 Alteon OS-Supported Enterprise SNMP Traps

Trap Name	Description
altSwTcpHoldDown	A altSwTcpHoldDown trap signifies that new TCP connection requests from a particular client will be blocked for a pre-determined amount of time since the rate of new TCP connections from that client has reached a pre-determined threshold.
altSwTempExceedThreshold	A altSwTempExceedThreshold trap signifies that the switch temperature has exceeded maximum safety limits.

Working with 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 9-9.

The examples in this section use the MIB name, but you can also use the OID.

Table 9-9 lists the MIBS used to perform operations associated with the GbESM Switch Image and Configuration files. These MIBS are contained within in the file “aosswitch.mib”

Table 9-9 MIBs for Switch Image and Configuration Files

MIB Name	MIB IOD
aqTftpServer	1.3.6.1.4.1872.2.5.1.1.7.1
aqTftpImage	1.3.6.1.4.1872.2.5.1.1.7.2
aqTftpImageFileName	1.3.6.1.4.1872.2.5.1.1.7.3
aqTftpCfgFileName	1.3.6.1.4.1872.2.5.1.1.7.4
aqTftpDumpFileName	1.3.6.1.4.1872.2.5.1.1.7.5
aqTftpAction	1.3.6.1.4.1872.2.5.1.1.7.6
aqTftpLastActionStatus	1.3.6.1.4.1872.2.5.1.1.7.7
aqTftpPort	1.3.6.1.4.1872.2.5.1.1.7.8

The following SNMP actions can be performed using the MIBs listed in Table 9-9.

- Load a new Switch image (boot or running) from a TFTP server
- Load a previously saved switch configuration from a TFTP server
- Save the switch configuration to a TFTP server
- Save a switch dump to a 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 TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the switch image resides:**

   ```
   Set aqTftpServer.0 "192.168.10.10"
   ```

2. **Set the area where the new image will be loaded:**

   ```
   Set aqTftpImage.0 "image2"
   ```

3. **Set the name of the image:**

   ```
   Set aqTftpImageFileName.0 "MyNewImage-1.img"
   ```

4. **Set the port for the TFTP data transfer. Enter 1 to perform the transfer across the data port. Enter 2 to perform the transfer across the management port:**

   ```
   Set aqTftpPort.0 "1"
   ```

5. **Initiate the transfer. To transfer a switch image, enter 2 (gtimg):**

   ```
   Set aqTftpAction.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 TFTP server address where the switch Configuration File resides:**

   ```
   Set aqTftpServer.0 "192.168.10.10"
   ```

2. **Set the name of the configuration file:**

   ```
   Set aqTftpCfgFileName.0 "MyRunningConfig.cfg"
   ```

3. **Set the port for the TFTP data transfer. Enter 1 to perform the transfer across the data port. Enter 2 to perform the transfer across the management port.**

   ```
   Set aqTftpPort.0 "1"
   ```

4. **Initiate the transfer. To restore a running configuration, enter 3:**

   ```
   Set aqTftpAction.0 "3"
   ```

Saving the switch configuration

To save the switch configuration to a TFTP server follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the configuration file is saved:**

```
Set aqTftpServer.0 "192.168.10.10"
```

2. **Set the name of the configuration file:**

```
Set aqTftpCfgFileName.0 "MyRunningConfig.cfg"
```

3. **Set the port for the TFTP data transfer. Enter 1 to perform the transfer across the data port. Enter 2 to perform the transfer across the management port.**

```
Set aqTftpPort.0 "1"
```

4. **Initiate the transfer. To save a running configuration file, enter 4:**

```
Set aqTftpAction.0 "4"
```

Saving a switch dump

To save a switch dump to a TFTP, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. **Set the TFTP server address where the configuration will be saved:**

```
Set aqTftpServer.0 "192.168.10.10"
```

2. **Set the name of dump file:**

```
Set aqTftpDumpFileName.0 "MyDumpFile.dmp"
```

3. **Set the port for the TFTP data transfer. Enter 1 to perform the transfer across the data port. Enter 2 to perform the transfer across the management port.**

```
Set aqTftpPort.0 "1"
```

4. **Initiate the transfer. To save a dump file, enter 5:**

```
Set aqTftpAction.0 "5"
```

Glossary

DIP (Destination IP Address)
The destination IP address of a frame.

Dport (Destination Port)
The destination port (application socket: for example, http-80/https-443/DNS-53)

NAT (Network Address Translation)
Any time an IP address is changed from one source IP or destination IP address to another address, network address translation can be said to have taken place. In general, half NAT is when the destination IP or source IP address is changed from one address to another. Full NAT is when both addresses are changed from one address to another. No NAT is when neither source nor destination IP addresses are translated. Virtual server-based load balancing uses half NAT by design, because it translates the destination IP address from the Virtual Server IP address, to that of one of the real servers.

Preemption
In VRRP, preemption will cause a Virtual Router that has a lower priority to go into backup should a peer Virtual Router start advertising with a higher priority.

Priority
In VRRP, the value given to a Virtual Router to determine its ranking with its peer(s). Minimum value is 1 and maximum value is 254. Default is 100. A higher number will win out for master designation.

Proto (Protocol)
The protocol of a frame. Can be any value represented by a 8-bit value in the IP header adherent to the IP specification (for example, TCP, UDP, OSPF, ICMP, and so on.)

RIP (Real Server)
Real Server IP Address. An IP addresses that the switch load balances to when requests are made to a Virtual Server IP address (VIP).

SIP (Source IP Address)
The source IP address of a frame.

SPort (Source Port)
The source port (application socket: for example, HTTP-80/HTTPS-443/DNS-53).

Tracking

In VRRP, a method to increase the priority of a virtual router and thus master designation (with preemption enabled). Tracking can be very valuable in an active/active configuration.

You can track the following:

- ifs: Active IP interfaces on the GbE Switch Module (increments priority by 2 for each)
- ports: Active ports on the same VLAN (increments priority by 2 for each)
- vrs: Number of virtual routers in master mode on the switch

VIR (Virtual Interface Router)

A VRRP address that is an IP interface address shared between two or more virtual routers.

Virtual Router

A shared address between two devices utilizing VRRP, as defined in RFC 2338. One virtual router is associated with an IP interface. This is one of the IP interfaces that the switch is assigned. All IP interfaces on the GbE Switch Module must be in a VLAN. If there is more than one VLAN defined on the GbE Switch Module, then the VRRP broadcasts will only be sent out on the VLAN of which the associated IP interface is a member.

VRID (Virtual Router Identifier)

In VRRP, a value between 1 and 255 that is used by each virtual router to create its MAC address and identify its peer for which it is sharing this VRRP address. The VRRP MAC address as defined in the RFC is 00-00-5E-00-01-{VRID}. If you have a VRRP address that two switches are sharing, then the VRID number needs to be identical on both switches so each virtual router on each switch knows whom to share with.

VRRP (Virtual Router Redundancy Protocol)

A protocol that acts very similarly to Cisco's proprietary HSRP address sharing protocol. The reason for both of these protocols is so devices have a next hop or default gateway that is always available. Two or more devices sharing an IP interface are either advertising or listening for advertisements. These advertisements are sent via a broadcast message to an address such as 224.0.0.18.

With VRRP, one switch is considered the master and the other the backup. The master is always advertising via the broadcasts. The backup switch is always listening for the broadcasts. Should the master stop advertising, the backup will take over ownership of the VRRP IP and MAC addresses as defined by the specification. The switch announces this change in ownership to the devices around it by way of a Gratuitous ARP, and advertisements. If the backup switch didn't do the Gratuitous ARP the Layer 2 devices attached to the switch would not know that the MAC address had moved in the network. For a more detailed description, refer to RFC 2338.