



Alteon OSTM **Command Reference**

Layer 2/3 GbE Switch Module for IBM BladeCenter[®]
Version 1.5

Part Number: BMD00029, April 2008

BLADE
N E T W O R K
T E C H N O L O G I E S

2350 Mission College Blvd.
Suite 600
Santa Clara, CA 95054
www.bladenetwork.net

Copyright © 2008 Blade Network Technologies, Inc., 2350 Mission College Blvd., Suite 600, Santa Clara, California, 95054, USA. All rights reserved. Part Number: BMD00029.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Blade Network Technologies, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

Blade Network Technologies, Inc. reserves the right to change any products described herein at any time, and without notice. Blade Network Technologies, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Blade Network Technologies, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Blade Network Technologies, Inc.

Originated in the USA.

Alteon OS, and Alteon are trademarks of Nortel Networks, Inc. in the United States and certain other countries. Cisco[®] and EtherChannel[®] are registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Contents

Preface 13

Who Should Use This Book 14

How This Book Is Organized 15

Typographic Conventions 16

How to Get Help 17

The Command Line Interface 19

Connecting to the Switch 20

 Management Module Setup 20

 Factory-Default vs. MM assigned IP Addresses 20

 Default Gateway 21

 Configuring management module for switch access 21

 Connecting to the Switch via Telnet 23

 Running Telnet 23

 Establishing an SSH Connection 24

 Running SSH 25

Accessing the Switch 26

Setup Versus CLI 28

Command Line History and Editing 29

Idle Timeout 29

First-Time Configuration 31

Using the Setup Utility 32

 Information Needed For Setup 32

 Starting Setup When You Log In 32

 Stopping and Restarting Setup Manually 34

 Stopping Setup 34

 Restarting Setup 34

 Setup Part 1: Basic System Configuration 34

 Setup Part 2: Port Configuration 36

Setup Part 3: VLANs	38
Setup Part 4: IP Configuration	39
IP Interfaces	39
Default Gateways	40
IP Routing	41
Setup Part 5: Final Steps	41
Optional Setup for Telnet Support	42
Setting Passwords	43
Changing the Default Administrator Password	43
Changing the Default User Password	45

Menu Basics 47

The Main Menu	48
Menu Summary	49
Global Commands	50
Command Line History and Editing	53
Command Line Interface Shortcuts	54
Command Stacking	54
Command Abbreviation	54
Tab Completion	54

The Information Menu 55

Information Menu	56
System Information	58
SNMPv3 System Information Menu	59
SNMPv3 USM User Table Information	61
SNMPv3 View Table Information	62
SNMPv3 Access Table Information	63
SNMPv3 Group Table Information	64
SNMPv3 Community Table Information	64
SNMPv3 Target Address Table Information	65
SNMPv3 Target Parameters Table Information	66
SNMPv3 Notify Table Information	67
SNMPv3 Dump Information	68
BladeCenter Chassis Information	69
General System Information	70
Show Recent Syslog Messages	72
User Status	73
Layer 2 Information	74

FDB Information	76
Show All FDB Information	77
Clearing Entries from the Forwarding Database	77
Link Aggregation Control Protocol Information	78
Show all LACP Information	78
802.1X Information	80
Spanning Tree Information	82
RSTP/MSTP Information	85
Common Internal Spanning Tree Information	88
Trunk Group Information	91
VLAN Information	91
Layer 3 Information	93
IP Routing Information	95
Show All IP Route Information	96
ARP Information	98
Show All ARP Entry Information	99
ARP Address List Information	99
BGP Information	100
BGP Peer information	100
BGP Summary information	101
Show all BGP Information	101
OSPF Information	102
OSPF General Information	103
OSPF Interface Information	104
OSPF Database Information	104
OSPF Information Route Codes	106
Routing Information Protocol Information	107
RIP Routes Information	107
Show RIP User Configuration	108
ECMP Static Routes Information	108
IP Information	109
IGMP Multicast Group Information	110
IGMP Group Information	111
IGMP Multicast Router Port Information	111
IGMP Mrouter Information	112
VRRP Information	113
Quality of Service Information	114
802.1p Information	114
Access Control List Information	116
Link Status Information	117
Port Information	118

Fiber Port Transceiver Status 119
Information Dump 119

The Statistics Menu 121

Statistics Menu 121
Port Statistics 123
 802.1X Authenticator Statistics 124
 802.1X Authenticator Diagnostics 125
 Bridging Statistics 127
 Ethernet Statistics 129
 Interface Statistics 132
 Interface Protocol Statistics 134
 Link Statistics 134
Layer 2 Statistics 135
 FDB Statistics 135
 LACP Statistics 136
Layer 3 Statistics 137
 IP Statistics 140
 Route Statistics 142
 ARP statistics 142
 DNS Statistics 143
 ICMP Statistics 143
 TCP Statistics 146
 UDP Statistics 148
 IGMP Statistics 149
 OSPF Statistics 150
 OSPF Global Statistics 151
 VRRP Statistics 155
 Routing Information Protocol Statistics 156
Management Processor Statistics 157
 MP Packet Statistics 158
 TCP Statistics 159
 UCB Statistics 159
 CPU Statistics 160
ACL Statistics 161
 ACL Statistics 161
 ACL Meter Statistics 162
SNMP Statistics 163
NTP Statistics 167
Statistics Dump 168

The Configuration Menu 169

Configuration Menu 170

Viewing, Applying, and Saving Changes 172

Viewing Pending Changes 172

Applying Pending Changes 172

Saving the Configuration 173

System Configuration 174

System Host Log Configuration 177

SSH Server Configuration 178

RADIUS Server Configuration 179

TACACS+ Server Configuration 181

LDAP Server Configuration 184

NTP Server Configuration 186

System SNMP Configuration 187

SNMPv3 Configuration 189

User Security Model Configuration 191

SNMPv3 View Configuration 192

View-based Access Control Model Configuration 193

SNMPv3 Group Configuration 195

SNMPv3 Community Table Configuration 196

SNMPv3 Target Address Table Configuration 197

SNMPv3 Target Parameters Table Configuration 198

SNMPv3 Notify Table Configuration 199

System Access Configuration 200

Management Networks Configuration 202

User Access Control Configuration 203

System User ID Configuration 204

Strong Password Configuration 205

HTTPS Access Configuration 206

Port Configuration 207

Port Link Configuration 209

Temporarily Disabling a Port 210

Port ACL Configuration 210

ACL Port Metering Menu 211

Re-Mark Menu 212

Re-Marking In-Profile Menu 213

Update User Priority Menu 214

Re-Marking Out-of-Profile Menu 215

Layer 2 Configuration 216

802.1X Configuration	218
802.1X Global Configuration	219
802.1X Guest VLAN Configuration	221
802.1X Port Configuration	222
Rapid Spanning Tree Protocol/ Multiple Spanning Tree Protocol Configuration	224
Common Internal Spanning Tree Configuration	226
CIST Bridge Configuration	227
CIST Port Configuration	228
Spanning Tree Configuration	230
Spanning Tree Bridge Configuration	232
Spanning Tree Port Configuration	234
Forwarding Database Configuration	236
Static FDB Configuration	237
Trunk Configuration	238
IP Trunk Hash Configuration	239
IP Trunk Hash	239
LACP Configuration	241
LACP Port Configuration	242
Layer 2 Failover Configuration	243
Failover Trigger Configuration	244
Auto Monitor Configuration	245
VLAN Configuration	246
Protocol-based VLAN Configuration	248
Private VLAN Configuration	250
VLAN Bandwidth Management Configuration	251
Layer 3 Configuration	252
IP Interface Configuration	254
Default Gateway Configuration	255
IP Static Route Configuration	257
IP Multicast Route Configuration	258
ARP Configuration	259
ARP Static Configuration	260
IP Forwarding Configuration	261
Network Filter Configuration	262
Routing Map Configuration	263
IP Access List Configuration	265
Autonomous System Filter Path	266
Routing Information Protocol Configuration	267
Routing Information Protocol Interface Configuration	268

Open Shortest Path First Configuration	270
Area Index Configuration	272
OSPF Summary Range Configuration	273
OSPF Interface Configuration	274
OSPF Virtual Link Configuration	276
OSPF Host Entry Configuration	277
OSPF Route Redistribution Configuration	278
OSPF MD5 Key Configuration	279
Border Gateway Protocol Configuration	280
BGP Peer Configuration	282
BGP Redistribution Configuration	284
BGP Aggregation Configuration	285
IGMP Configuration	286
IGMP Snooping Configuration	287
IGMP Version 3 Configuration	288
IGMP Relay Configuration	289
IGMP Relay Multicast Router Configuration	290
IGMP Static Multicast Router Configuration	291
IGMP Filtering Configuration	292
IGMP Filter Definition	293
IGMP Filtering Port Configuration	294
IGMP Advanced Configuration	295
Domain Name System Configuration	296
Bootstrap Protocol Relay Configuration	297
VRRP Configuration	298
Virtual Router Configuration	300
Virtual Router Priority Tracking Configuration	302
Virtual Router Group Configuration	303
Virtual Router Group Priority Tracking Configuration	305
VRRP Interface Configuration	306
VRRP Tracking Configuration	307
Quality of Service Configuration	308
802.1p Configuration	309
DSCP Configuration	310
Access Control List Configuration	311
ACL Configuration	312
Ethernet Filtering Configuration	313
IP version 4 Filtering Configuration	314
TCP/UDP Filtering Configuration	315
Packet Format Filtering Configuration	316
ACL Block Menu	317

- ACL Group Configuration 318
- Port Mirroring Configuration 319
 - Port-Mirroring Configuration 320
- Setup 321
- Dump 321
- Saving the Active Switch Configuration 322
- Restoring the Active Switch Configuration 322

The Operations Menu 323

- Operations Menu 324
 - Operations-Level Port Options 326
 - Operations-Level Port 802.1X Options 327
 - Operations-Level VRRP Options. 328
 - Operations-Level IP Options 329
 - Operations-Level BGP Options 329
 - Protected Mode Options 330

The Boot Options Menu 333

- Boot Menu 334
- Scheduled Reboot of the Switch 334
 - Scheduled Reboot Menu 334
- Updating the Switch Software Image 335
 - Loading New Software to Your Switch 335
 - Using the BBI 335
 - Using the AOS CLI 337
 - Selecting a Software Image to Run 338
 - Uploading a Software Image from Your Switch 339
- Selecting a Configuration Block 340
- Resetting the Switch 341
 - Accessing the ISCLI 341

The Maintenance Menu 343

- Maintenance Menu 344
 - System Maintenance 346
 - Forwarding Database Maintenance 347
 - Debugging Options 348
 - ARP Cache Maintenance 349
 - IP Route Manipulation 350

IGMP Maintenance	351
IGMP Group Maintenance	351
IGMP Multicast Routers Maintenance	352
Uuencode Flash Dump	353
TFTP System Dump Put	354
Clearing Dump Information	354
Panic Command	355
Unscheduled System Dumps	355

Alteon OS Syslog Messages 357

Alteon OS SNMP Agent 369

Working with Switch Images and Configuration Files	372
Loading a new switch image	373
Loading a saved switch configuration	374
Saving the switch configuration	374
Saving a switch dump	375

Glossary 377

Index 1

Preface

The Alteon OS *Command Reference* describes how to configure and use the Alteon OS software with your Layer 2/3 GbE Switch Module.

For documentation on installing the switches physically, see the *Installation Guide* for your GbE Switch Module. For details about configuration and operation of your GbE Switch Module, see the Alteon OS *Application Guide*.

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. It also depicts on-screen computer output and prompts.	View the <code>readme.txt</code> file. 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. This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# telnet <IP address> Read your <i>User's Guide</i> 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 Layer 2/3 GbE Switch Module for IBM BladeCenter *Installation Guide*.

CHAPTER 1

The Command Line Interface

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

The extensive 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 its internal port 15 (MGT1) and port 16 (MGT2), which you can access through the Ethernet port on the management module. The factory default settings will permit *only* management and control access to the switch module through the 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 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 192.168.70.1xx, where xx corresponds to the number of the bay into which each GbE Switch Module is installed, as shown in the following table:

Table 1-1 GbESM IP addresses, based on switch-module bay numbers

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

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

Default Gateway

The default Gateway IP address determines where packets with a destination address outside the current subnet 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 > Configuration** from the navigation pane on the left, and enter the default Gateway IP address (for example, 192.168.70.125). Click **Save**.

Configuring management module for switch access

Complete the following initial configuration steps:

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

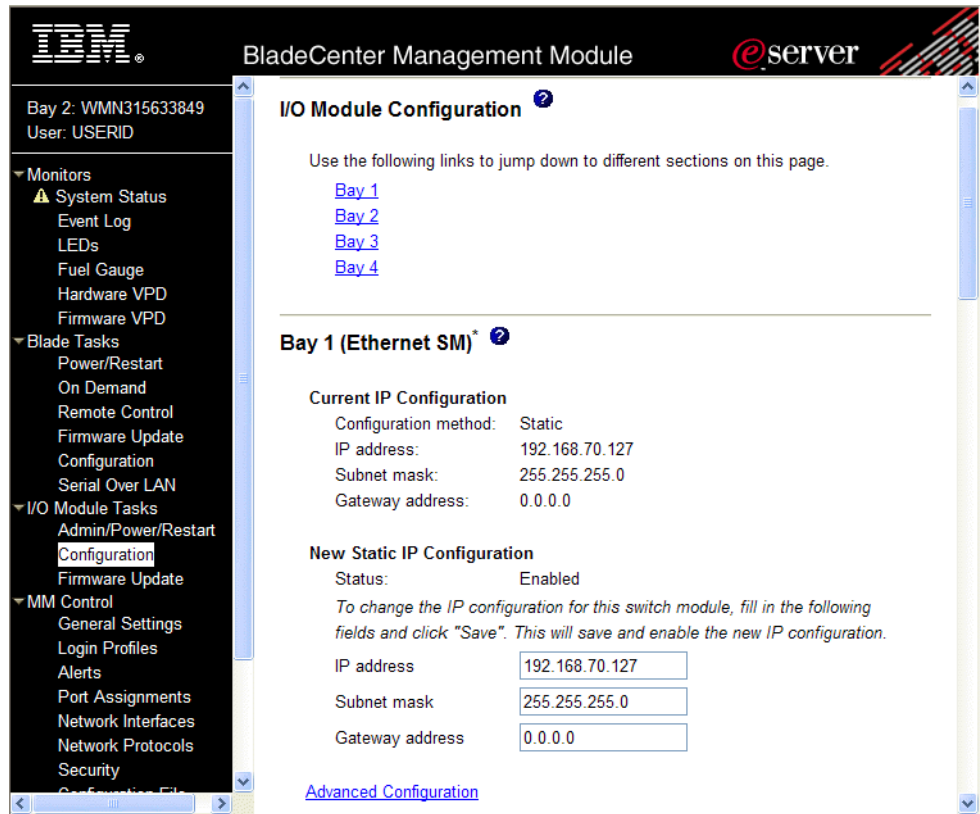


Figure 1-1 Switch management on the BladeCenter management module

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 (available in Director release 4.21)

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

5. Enable the following features in the management module:

- External Ports (**I/O Module Tasks > Admin/Power/Restart > Advance Setup**)
- External management over all ports (**Configuration > Advanced Configuration**)
This setting is required if you want to access the management network through the 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 **Advanced Configuration > Advanced Setup**, enable “Preserve new IP configuration on all switch resets,” to retain the switch’s IP interface when you restore factory defaults. This setting preserves the management port’s IP address in the management module’s memory, so you maintain connectivity to the management module after a reset.

You can now start a Telnet session, Browser-Based Interface (Web) session, a Secure Shell session, or a secure HTTPS session to the 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 > Configuration** from the navigation pane on the left. Select a bay number and click **Advanced Configuration > Start Telnet/Web Session > Start Telnet Session**. A Telnet window opens a connection to the Switch Module (requires Java 1.4 Plug-in).

Once that you have configured the 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 27](#).

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) are not 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 -l 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 43](#).

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. The Operator can reset ports, except the management ports.	oper
Administrator	The superuser Administrator has complete access to all menus, information, and configuration commands on the 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 47.](#)”

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 174.](#)

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 connect 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:

```
Nortel Layer2-3 GbE Switch Module  
18:44:05 Wed Jan 3, 2007
```

```
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 340](#).

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, Spanning Tree, Port Speed/Mode,
VLANs, and IP interfaces. [type Ctrl-C to abort "Set Up"]
-----
```

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 *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 [2007]:
```

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 revert to default values. Use `/cfg/sys/date` and `/cfg/sys/time` to re-enter the current date and time.

The system displays the date and time settings:

```
System clock set to 18:55:36 Wed Jan 3, 2007.
```

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, 2007.
```

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:
Will you configure VLANs and VLAN tagging for ports? [y/n] y
Enter port (INT1-14, MGT1-2, EXT1-6):
```

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 38](#).

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 (INT1-14, MGT1-2, EXT1-6):
```

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 39](#).

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

```
VLAN Config:
Enter VLAN number from 2 to 4094, 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 39](#).

2. Enter the new VLAN name at the prompt:

```
Current 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. 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.

4. Configure Spanning Tree Group membership for the VLAN:

```
Spanning Tree Group membership:
Current Spanning Tree Group index: 1
Enter new Spanning Tree Group index [1-127]:
```

5. The system prompts you to configure the next VLAN:

```
VLAN Config:
Enter VLAN number from 2 to 4094, 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 wish to configure. To skip IP interface configuration, press <Enter> without typing an interface number and go to [“Default Gateways” on page 40](#).

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 [1-4090]:
```

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 41](#).

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**. To keep the current setting, press <Enter>.

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 43](#).

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/access/tnet
```

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

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

Setting Passwords

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

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

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

Changing the Default Administrator Password

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

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

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

```
Main# /cfg
```

The Configuration Menu is displayed.

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

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

```
>> Configuration# sys
```

The System Menu is displayed.

```
[System Menu]
  syslog - Syslog Menu
  sshd   - SSH Server Menu
  radius - RADIUS Authentication Menu
  tacacs+ - TACACS+ Authentication Menu
  ldap   - LDAP Authentication Menu
  ntp     - NTP Server Menu
  ssnmpp - System SNMP Menu
  access - System Access Menu
  date    - Set system date
  time    - Set system time
  timezone - Set system timezone (daylight savings)
  olddst  - Set system DST for US
  dlight  - Set system daylight savings
  idle    - Set timeout for idle CLI sessions
  notice  - Set login notice
  e2e     - Enable/disable end-to-end flow control mode
  hgibp   - Enable/disable higig IBP
  bannr   - Set login banner
  hprompt - Enable/disable display hostname (sysName) in CLI prompt
  reminder - Enable/disable Reminders
  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
  userbbi - Enable/disable user configuration from BBI
  tnet    - Enable/disable Telnet access
  tnport  - Set Telnet server port number
  tport   - Set the TFTP Port for the system
  cur     - Display current system access configuration
```

5. **Select the administrator password.**

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

6. **Enter the current administrator password at the prompt:**

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

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

7. **Enter the new administrator password at the prompt:**

```
Enter new administrator password:
```

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

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

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

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

Changing the Default User Password

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

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

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

```
Main# cfg
```

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

```
>> Configuration# sys
```

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

```
>> System# access
```

5. Select the user password.

```
System# user/usrpw
```

6. Enter the current administrator password at the prompt.

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

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

7. Enter the new user password at the prompt:

```
Enter new user password:
```

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

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

9. Apply and save your changes:

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

CHAPTER 3

Menu Basics

The 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 short-cuts 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
revert apply
ping            traceroute    telnet          history
pushd           popd          who             chpass_p
chpass_s

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
? <i>command</i> or help	Provides more information about a specific command on the current menu. When used without the <i>command</i> 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 remove any configuration changes made since last apply .
revert apply	Remove pending or applied configuration changes between “save” commands. Use this command to remove any configuration changes made since last save .
exit or quit	Exit from the command line interface and log out.
ping	<p>Use this command to verify station-to-station connectivity across the network. The format is as follows:</p> <pre>ping <host name> <IP address> [tries (1-32)] [msec delay]]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the device, <i>tries</i> (optional) is the number of attempts (1-32), <i>msec delay</i> (optional) is the number of milliseconds between attempts. Configure the DNS parameters if specifying hostnames (see “Domain Name System Configuration” on page 296).</p>
tracert	<p>Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows:</p> <pre>tracert <host name> <IP address> [<max-hops (1-32)> [msec delay]]</pre> <p>Where <i>IP address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-16 devices), and <i>delay</i> (optional) is the number of milliseconds for wait for the response. As with ping, the DNS parameters must be configured if specifying hostnames.</p>
pwd	Display the command path used to reach the current menu.
verbose <i>n</i>	<p>Sets the level of information displayed on the screen:</p> <ul style="list-style-type: none"> 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. <p>When used without a value, the current setting is displayed.</p>
telnet	<p>This command is used to telnet out of the switch. The format is as follows:</p> <pre>telnet <host name> <IP address> [port]</pre>
history	This command displays the most recent commands.
pushd	Save the current menu path, so you can jump back to it using popd .
popd	Go to the menu path and position previously saved by using pushd .
who	Displays a list of users that are logged on to the switch.
chpass_p	Configures the password for the primary TACACS+ server.

Table 3-1 Description of Global Commands

Command	Action
chpass_s	Configures the password for the secondary TACACS+ server.

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 64 previously entered commands.
!!	Repeat the last entered command.
!<i>n</i>	Repeat the <i>n</i> th command shown on the history list.
<Ctrl-p>	(Also the up arrow key.) Recall the <i>previous</i> command from the history list. This can be used multiple times to work backward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the <i>next</i> command from the history list. This can be used multiple times to work forward through the last 64 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the <i>end</i> of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor <i>back</i> one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor <i>forward</i> one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	<i>Delete</i> one character at the cursor position.
<Ctrl-k>	<i>Kill</i> (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/12/stg 1/port
```

Command Abbreviation

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

```
Main# c/12/stg 1/po
```

Tab Completion

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

CHAPTER 4

The Information Menu

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

/info

Information Menu

```
[Information Menu]
sys      - System Information Menu
12       - Layer 2 Information Menu
13       - Layer 3 Information Menu
qos      - QoS Menu
acl      - Show ACL information
link     - Show link status
port     - Show port information
transcvr - Show Port Transceiver status
dump     - Dump all information
```

The information provided by each menu option is briefly described in [Table 4-1](#), with pointers to detailed information.

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage

sys

Displays the System Information Menu. For details, see [page 58](#).

12

Displays the Layer 2 Information Menu. For details, see [page 74](#).

13

Displays the Layer 3 Information Menu. For details, see [page 93](#).

qos

Displays the Quality of Service (QoS) Information Menu. For details, see [page 114](#).

acl

Displays the current configuration profile for each Access Control List (ACL) and ACL Group. For details, see [page 116](#).

link

Displays configuration information about each port, including:

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

For details, see [page 117](#).

Table 4-1 Information Menu Options (/info)

Command Syntax and Usage

port

Displays port status information, including:

- Port alias and number
- Whether the port uses VLAN Tagging or not
- Port Fast Forwarding status
- FDB Learning status
- Flooding of unknown destination MAC status
- Port VLAN ID (PVID)
- Port name
- VLAN membership

For details, see [page 118](#).

transcvr

Displays the status of the port transceiver module on each Fiber External Port.

For details, see [page 119](#).

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
chassis	- Show BladeCenter Chassis related information
general	- Show general system information
log	- Show last 100 syslog messages
user	- Show current user status
e2eshow	- Show E2E status
dump	- Dump all system information

The information provided by each menu option is briefly described in [Table 4-2](#), 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 59](#).

chassis

Displays information about the BladeCenter chassis. For details, see [page 69](#).

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 the management interface
- Hardware version and part number
- Software image file and version number
- Configuration name
- Log-in banner, if one is configured

For details, see [page 70](#).

log

Displays most recent syslog messages. For details, see [page 72](#).

user

Displays configured user names and their status. For details, see [page 73](#).

e2eshow

Displays End-to-End Flow Control information.

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

Command Syntax and Usage

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 61](#).

view

Displays information about view, sub-trees, mask and type of view. To view a sample, see [page 62](#).

access

Displays View-based Access Control information. To view a sample, see [page 63](#).

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

Command Syntax and Usage

group

Displays information about the group that includes, the security model, user name, and group name. To view a sample, see [page 64](#).

comm

Displays information about the community table information. To view a sample, see [page 64](#).

taddr

Displays the Target Address table information. To view a sample, see [page 65](#).

tparam

Displays the Target parameters table information. To view a sample, see [page 66](#).

notify

Displays the Notify table information. To view a sample, see [page 67](#).

dump

Displays all the SNMPv3 information. To view a sample, see [page 68](#).

/info/sys/snmpv3/usm
SNMPv3 USM User Table Information

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

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

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

Table 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
iso	1.3		included
vlv2only	1.3		included
vlv2only	1.3.6.1.6.3.15		excluded
vlv2only	1.3.6.1.6.3.16		excluded
vlv2only	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	Model	Level	ReadV	WriteV	NotifyV
vlv2grp	snmpv1	noAuthNoPriv	iso	iso	vlv2only
admingrp	usm	authPriv	iso	iso	iso

Table 4-6 SNMPv3 Access Table Information (/info/sys/snmpv3/access)

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

/info/sys/snmpv3/group

SNMPv3 Group Table Information

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

Sec Model	User Name	Group Name
-----	-----	-----
snmpv1	vlv2only	vlv2grp
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	vlv2only	vlv2trap

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 <code>snmpTargetAddrEntry</code> .
Transport Addr	Displays the transport addresses.
Port	Displays the SNMP UDP port number.
Taglist	This column contains a list of tag values which are used to select target addresses for a particular SNMP message.
Params	The value of this object identifies an entry in the <code>snmpTargetParamsTable</code> . The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address.

/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 <code>snmpTargeParamsEntry</code> .
MP Model	Displays the Message Processing Model used when generating SNMP messages using this entry.
User Name	Displays the <code>securityName</code> , which identifies the entry on whose behalf SNMP messages will be generated using this entry.
Sec Model	Displays the security model used when generating SNMP messages using this entry. The system may choose to return an <code>inconsistentValue</code> error if an attempt is made to set this variable to a value for a security model which the system does not support.
Sec Level	Displays the level of security used when generating SNMP messages using this entry.

/info/sys/snmpv3/notify
SNMPv3 Notify Table Information

Name	Tag
-----	-----
vlv2trap	vlv2trap

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

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

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

vacmSecurityToGroup Table:
Sec Model User Name Group Name
-----
snmpv1 v1v2only v1v2grp
usm adminmd5 admingrp
usm adminsha admingrp

snmpCommunity Table:
Index Name User Name Tag
-----

snmpNotify Table:
Name Tag
-----

snmpTargetAddr Table:
Name Transport Addr Port Taglist Params
-----

snmpTargetParams Table:
Name MP Model User Name Sec Model Sec Level
-----

```

info/sys/chassis

BladeCenter Chassis Information

IBM BladeCenter Chassis Related Information:

```
Switch Module Bay = 1
Chassis Type      = Enterprise
POST Results      = 0xff
```

Management Module Control -

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

```
Control Register           = 0x19
Extended Control Register  = 0x00
```

Management Module Status Reporting -

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

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

Chassis information includes details about the BladeCenter chassis and management module settings.

`/info/sys/general`

General System Information

```

System Information at 0:16:42 Wed Jan 3, 2007
Time zone: No timezone configured

Nortel Layer 2-3 GbE Switch Module

Switch is up 5 days, 2 hours, 16 minutes and 42 seconds.
Last boot: 0:00:47 Wed Jan 3, 2007 (power cycle)

MAC address: 00:11:58:ad:a3:00 Management IP Address (if 128):
10.90.90.97
Software Version 1.5.0 (FLASH image1), active configuration.

PCBA Part Number:      317857-A
FAB Number:            EL4512011
Serial Number:         YJ1WDW47N277
Manufacturing Date:
Hardware Revision:     0
Board Revision:        2
PLD Firmware Version:  1.0

Temperature Sensor 1 (Warning): 33.0 C (Warn at 77.0 C/
Recover at 72.0 C)
Temperature Sensor 2 (Shutdown): 32.0 C (Warn at 90.0 C/
Recover at 80.0 C)
Temperature Sensor 3 (Exhaust): 0.0 C
Temperature Sensor 4 (Inlet): 0.0 C

Switch is in I/O Module Bay 1

```

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

System information includes:

- System date and time
- Switch model
- Switch name and location
- Time of last boot
- MAC address of the switch management processor
- IP address of management IP interface

- Hardware version and part number
- Software image file and version number
- Configuration name
- Log-in banner, if one is configured

/info/sys/log

Show Recent Syslog Messages

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

Each syslog message has a criticality level associated with it, included in text form as a prefix to the log message. One of eight different prefixes is used, depending on the condition that the administrator is being notified of, as shown below.

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

/info/sys/user

User Status

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

This command displays the status of the configured usernames.

/info/l2

Layer 2 Information

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

The information provided by each menu option is briefly described in [Table 4-12](#), 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 76](#).

lacp

Displays the Link Aggregation Control Protocol Menu. For details, see [page 78](#).

8021x

Displays the 802.1X Information Menu. For details, see [page 80](#).

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 82](#).

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

Command Syntax and Usage

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 88](#).

trunk

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

For details, see [page 91](#).

vlan

Displays VLAN configuration information, including:

- VLAN Number
- VLAN Name
- Status
- Port membership of the VLAN

For details, see [page 91](#).

gen

Displays general Layer 2 information.

dump

Dumps all switch information available from the Layer 2 menu (10K or more, depending on your configuration).

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

/info/l2/fdb

FDB Information

[Forwarding Database Menu]	
<code>find</code>	- Show a single FDB entry by MAC address
<code>port</code>	- Show FDB entries on a single port
<code>trunk</code>	- Show FDB entries on a single trunk
<code>vlan</code>	- Show FDB entries on a single VLAN
<code>state</code>	- Show FDB entries by state
<code>dump</code>	- 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.

trunk *<trunk number>*

Displays all FDB entries for a particular trunk.

vlan *<VLAN number (1-4095)>*

Displays all FDB entries on a single VLAN.

state **unknown** | **forward** | **trunk**

Displays all FDB entries of a particular state.

dump

Displays all entries in the Forwarding Database. For more information, see [page 77](#).

`/info/12/fdb/dump`

Show All FDB Information

MAC address	VLAN	Port	Trnk	State
-----	----	----	----	-----
00:04:38:90:54:18	1	EXT4		FWD
00:09:6b:9b:01:5f	1	INT13		FWD
00:09:6b:ca:26:ef	4095	MGT1		FWD
00:0f:06:ec:3b:00	4095	MGT1		FWD
00:11:43:c4:79:83	1	EXT4		FWD
00:11:f9:36:71:00	4095	MGT1		FWD
00:13:0a:4d:3c:00	4095	MGT1		FWD

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.

Clearing Entries from the Forwarding Database

To clear the entire FDB, refer to [“Forwarding Database Maintenance” on page 347](#).

/info/12/lacp

Link Aggregation Control Protocol Information

[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 Link Aggregation Protocol (LACP) status information about each port on the GbE Switch Module.

Table 4-14 LACP Menu Options (/info/12/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 78](#).

/info/12/lacp/dump

Show all LACP Information

port	lacp	adminkey	operkey	selected	prio	attached aggr	trunk

INT1	active	30	30	y	32768	17	19
INT2	active	30	30	y	32768	17	19
INT3	off	19	19	n	32768	--	--
INT4	off	20	20	n	32768	--	--
...							

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/12/8021x

802.1X Information

```
System capability : Authenticator
System status    : disabled
Protocol version : 1
```

Port	Auth Mode	Auth Status	Authenticator PAE State	Backend 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 4-15 802.1X Parameter Descriptions (/info/l2/8021x)

Parameter	Description
Port	Displays each port's alias.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ initialize ■ request ■ response ■ success ■ fail ■ timeout ■ idle

/info/12/stg

Spanning Tree Information

```

-----
upfast disabled, update 40
Pvst+ compatibility mode enabled
-----

Spanning Tree Group 1: On (STP/PVST+)
VLANs: 1 10

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8000 00:16:60:f9:1e:00      0 (null)   2    20    15

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

Port  Priority  Cost  FastFwd  State  Designated Bridge  Des Port
-----
INT1      0      0      n  FORWARDING  *
INT2      0      0      n  FORWARDING  *
INT3      0      0      n  FORWARDING  *
INT4      0      0      n  FORWARDING  *
INT5      0      0      n  FORWARDING  *
INT6      0      0      n  FORWARDING  *
INT7      0      0      n  FORWARDING  *
INT8      0      0      n  FORWARDING  *
INT9      0      0      n  DISABLED    *
INT10     0      0      n  FORWARDING  *
INT11     0      0      n  FORWARDING  *
INT12     0      0      n  FORWARDING  *
INT13     0      0      n  FORWARDING  *
INT14     0      0      n  FORWARDING  *
EXT1     128     2      n  DISABLED
EXT2     128     2      n  DISABLED
EXT3     128     2      n  FORWARDING  8000-00:16:60:f9:1e:00  8013
EXT4     128    4!      n  FORWARDING  8000-00:16:60:f9:1e:00  8014
EXT5     128     2      n  DISABLED
EXT6     128     2      n  DISABLED

* = STP turned off for this port.
! = Automatic path cost.

```

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

The switch software uses the IEEE 802.1D Spanning Tree Protocol (STP). 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 4-16 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 4-16 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.
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 identifier of the port on the Designated Bridge to which this port is connected.

/info/12/stg

RSTP/MSTP Information

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

Current Root:          Path-Cost  Port Hello MaxAge FwdDel
8000 00:11:58:ae:39:00      0    EXT4      2    20    15

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

Port  Prio  Cost      State  Role Designated Bridge      Des Port  Type
-----
INT1   0      0    DSB  *
INT2   0      0    DSB  *
INT3   0      0    FWD  *
INT4   0      0    DSB  *
INT5   0      0    DSB  *
INT6   0      0    DSB  *
INT7   0      0    DSB  *
INT8   0      0    DSB  *
INT9   0      0    DSB  *
INT10  0      0    DSB  *
INT11  0      0    DSB  *
INT12  0      0    DSB  *
INT13  0      0    DSB  *
INT14  0      0    DSB  *
EXT1  128    2000    FWD  DESG 8000-00:11:58:ae:39:00  8011    P2P
EXT2  128    2000    DISC BKUP 8000-00:11:58:ae:39:00  8011    P2P
EXT3  128    2000    FWD  DESG 8000-00:11:58:ae:39:00  8013    P2P
EXT4  128   20000    DISC BKUP 8000-00:11:58:ae:39:00  8013    Shared
EXT5  128    2000    FWD  DESG 8000-00:11:58:ae:39:00  8011    P2P
EXT6  128    2000    FWD  DESG 8000-00:11:58:ae:39:00  8011    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.

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 224](#)), 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 4-17 RSTP/MSTP Parameter Descriptions

Parameter	Description
Current Root	The Current Root shows information about the root bridge for the Spanning Tree. Information includes the priority (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.
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).

Table 4-17 RSTP/MSTP Parameter Descriptions (Continued)

Parameter	Description
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	Shared			
EXT5	128	20000	FWD	DESG	8000-00:11:58:ae:39:00	8011	2	P2P			
EXT6	128	20000	FWD	DESG	8000-00:11:58:ae:39:00	8011	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 4-18 CIST Parameter Descriptions

Parameter	Description
CIST Root	The CIST Root shows information about the root bridge for the Common Internal Spanning Tree (CIST). Values on this row of information refer to the CIST root.
CIST Regional Root	The CIST Regional Root shows information about the root bridge for this MSTP region. Values on this row of information refer to the regional root.
Priority (bridge)	The bridge priority parameter controls which bridge on the network will become the STP root bridge.
Hello	The hello time parameter specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
MaxAge	The maximum age parameter specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigure the STP network.
FwdDel	The forward delay parameter specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
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 CIST 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, port state:
  EXT1: STG 1 forwarding
  EXT2: STG 1 forwarding
```

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

NOTE – If Spanning Tree Protocol on any port in the trunk group is set to *forwarding*, the remaining ports in the trunk group will also be set to *forwarding*.

/info/l2/vlan

VLAN Information

VLAN	Name	Status	Bandwidth	MGT	Ports
1	Default VLAN	ena	ena	dis	INT1-INT14 EXT1-EXT6
10	VLAN 10	ena	ena	dis	INT1
11	VLAN 11	ena	ena	dis	EXT3
30	VLAN 30	ena	ena	dis	EXT4
4095	Mgmt VLAN	ena	ena	ena	INT1-INT14 MGT1 MGT2
Private-VLAN	Type	Mapped-To	Status	Ports	
1000	primary	1001-1014	ena	EXT1	EXT2
1001	isolated	1000	ena	INT1	
1002	community	1000	ena	INT2	
1003	community	1000	ena	INT3	

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
- VLAN Status
- Bandwidth management status (enabled/disabled)
- Management status (enabled/disabled)
- Port membership of the VLAN
- Protocol-based VLAN information
- Private VLAN configuration

/info/l3

Layer 3 Information

[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
ecmp	- Show ECMP static routes information
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 4-19](#), with pointers to detailed information.

Table 4-19 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 95](#).

arp

Displays the Address Resolution Protocol (ARP) Information Menu. For details, see [page 98](#).

bgp

Displays BGP Information Menu. To view menu options, see [page 100](#).

ospf

Displays OSPF routing Information Menu. For details, see [page 102](#).

rip

Displays Routing Information Protocol Menu. For details, see [page 107](#).

ecmp

Displays information about ECMP static routes. For details, see [page 108](#).

Table 4-19 Layer 3 Menu Options (/info/l3)

Command Syntax and Usage

ip

Displays IP Information. For details, see [page 109](#).

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 110](#).

vrrp

Displays the VRRP Information Menu. For details, see [page 113](#).

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 4-20 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 4-21 on page 96](#).

tag **fixed** | **static** | **addr** | **rip** | **ospf** | **bgp** | **broadcast** | **martian** | **multicast**
Displays routes of a single tag. For a description of IP routing types, see [Table 4-22 on page 97](#).

if <interface number (1-128)>
Displays routes on a single interface.

dump
Displays all routes configured in the switch. For more information, see [page 96](#).

/info/13/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 4-21 IP Routing Type Parameters

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

The following table describes the Tag parameters.

Table 4-22 IP Routing Tag Parameters

Parameter	Description
fixed	The address belongs to a host or subnet attached to the switch.
static	The address is a static route which has been configured on the 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.
multicast	Indicates a multicast address.

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

The ARP information includes IP address and MAC address of each entry, address status flags (see [Table 4-23 on page 98](#)), VLAN and port for the address, and port referencing information.

Table 4-23 ARP Information Menu Options (/info/l3/arp)

Command Syntax and Usage

find <IP address (such as, 192.4.17.101)>
Displays a single ARP entry by IP address.

port <port alias or number>
Displays the ARP entries on a single port.

vlan <VLAN number (1-4095)>
Displays the ARP entries on a single VLAN.

addr
Displays the ARP address list: IP address, IP mask, MAC address, and VLAN flags.

dump
Displays all ARP entries. including:

- IP address and MAC address of each entry
- Address status flag (see below)
- The VLAN and port to which the address belongs
- The ports which have referenced the address (empty if no port has routed traffic to the IP address shown)

For more information, see [page 99](#).

`/info/13/arp/dump`

Show All ARP Entry Information

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

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 4-24 ARP Dump Flag Parameters

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

`/info/13/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

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

Table 4-25 BGP Peer Information Menu Options (/info/l3/bgp))

Command Syntax and Usage

peer

Displays BGP peer information. See [page 100](#) for a sample output.

summary

Displays peer summary information such as AS, message received, message sent, up/down, state. See [page 101](#) for a sample output.

dump

Displays the BGP routing table. See [page 101](#) for a sample output.

/info/l3/bgp/peer

BGP Peer information

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

```
BGP Peer Information:

3: 2.1.1.1          , version 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/13/bgp/summary

BGP Summary information

Following is an example of the information that /info/13/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/13/bgp/dump

Show all BGP Information

Following is an example of the information that /info/13/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 rmap; 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 4-26 OSPF Information Menu options (/info/l3/ospf)

Command Syntax and Usage

general

Displays general OSPF information. See [page 103](#) 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 104](#) 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 104](#).

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 4-26 OSPF Information Menu options (/info/l3/ospf)

Command Syntax and Usage

routes

Displays OSPF routing table. See [page 106](#) 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 4-27 OSPF Database Information Menu Options (/info/l3/ospf/dbase)

Command Syntax and Usage

advrtr <router-id (A.B.C.D)>

Takes advertising router as a parameter. Displays all the Link State Advertisements (LSAs) in the LS database that have the advertising router with the specified router ID, for example: 20.1.1.1.

asbrsum <adv-rtr (A.B.C.D)> / <link_state_id (A.B.C.D)> / <self>

Displays ASBR summary LSAs. The usage of this command is as follows:

- 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.
-

Table 4-27 OSPF Database Information Menu Options (/info/l3/ospf/dbase)

Command Syntax and Usage

dbsumm

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

- 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 `asbrsumm`.

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 `asbrsumm`.

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 `asbrsumm`.

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 `asbrsumm`.

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 `asbrsumm`.

all

Displays all the LSAs.

/info/13/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 Information

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

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

Table 4-28 RIP Information Menu Options (/info/l3/rip)

Command Syntax and Usage

routes

Displays RIP routes. For more information, see [page 107](#).

dump *<interface number or zero for all IFs>*

Displays RIP user's configuration. For more information, see [page 108](#).

/info/l3/rip/routes

RIP Routes Information

>> IP Routing# /info/l3/rip/routes
30.1.1.0/24 directly connected
3.0.0.0/8 via 30.1.1.11 metric 4
4.0.0.0/16 via 30.1.1.11 metric 16
10.0.0.0/8 via 30.1.1.2 metric 3
20.0.0.0/8 via 30.1.1.2 metric 2

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

/info/l3/rip/dump <interface number> Show 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/ecmp ECMP Static Routes Information

```

Current ecmp static routes:

```

Destination	Mask	Gateway	If	GW Status
10.10.1.1	255.255.255.255	10.100.1.1	1	up
		10.200.2.2	1	down
10.20.2.2	255.255.255.255	10.233.3.3	1	up
10.20.2.2	255.255.255.255	10.234.4.4	1	up
10.20.2.2	255.255.255.255	10.235.5.5	1	up

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

/info/l3/ip

IP Information

```

IP information:
  AS number 0

Interface information:
  1: 10.200.30.3      255.255.0.0      10.200.255.255, vlan 1, up
  128: 10.90.90.97    255.255.255.0    10.90.90.255,    vlan 4095, up

Default gateway information: metric strict
  1: 10.200.1.1,      vlan any,  up

Current BOOTP relay settings: OFF
  0.0.0.0, 0.0.0.0

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

Current network filter settings:
  none

Current route map settings:

```

IP information includes:

- IP interface information: Interface number, IP address, subnet mask, broadcast address, VLAN number, and operational status.
- Default gateway information: Metric for selecting which configured gateway to use, gateway number, IP address, and health status
- BootP relay settings
- IP forwarding settings, including the forwarding status of directed broadcasts, and the status of ICMP re-directs
- Network filter settings
- Route map 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
trunk	- Show groups on a single trunk
detail	- Show detail of a single group by IP group address
dump	- Show all groups

Table 4-29 describes the commands used to display information about IGMP groups learned by the switch.

Table 4-29 IGMP Multicast Group Information Menu Options (/info/l3/igmp)

Command Syntax and Usage

mrouter

Displays IGMP Multicast Router menu. To view menu options, see [page 111](#).

find <IP address>

Displays a single IGMP multicast group by its IP address.

vlan <VLAN number>

Displays all IGMP multicast groups on a single VLAN.

port <port number or alias>

Displays all IGMP multicast groups on a single port.

trunk <Trunk Group number>

Displays all IGMP multicast groups on a single trunk group.

detail <IP address>

Displays details about IGMP multicast groups, including source and timer information.

dump

Displays information for all multicast groups.

info/l3/igmp/dump

IGMP Group Information

Note: Local groups (224.0.0.x) are not snooped/relayed and will not appear.							
Source	Group	VLAN	Port	Version	Mode	Expires	Fwd
10.1.1.1	232.1.1.1	2	EXT4	V3	INC	4:16	Yes
10.1.1.5	232.1.1.1	2	EXT4	V3	INC	4:16	Yes
*	232.1.1.1	2	EXT4	V3	INC	-	No
10.10.10.43	235.0.0.1	9	EXT1	V3	INC	2:26	Yes
*	236.0.0.1	9	EXT1	V3	EXC	-	Yes

IGMP Group information includes:

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

/info/l3/igmp/mrouter

IGMP Multicast Router Port Information

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

Table 4-30 describes the commands used to display information about multicast routers (Mrouters) learned through IGMP Snooping.

Table 4-30 IGMP Mrouter Information Menu Options (/info/igmp/mrouter)

Command Syntax and Usage

vlan <VLAN number>

Displays the multicast router ports configured or learned on the selected VLAN.

dump

Displays information for all multicast groups learned by the switch.

info/13/igmp/mrouter/dump

IGMP Mrouter Information

VLAN	Port	Version	Expires	Max Query Resp. Time	QRV	QQIC
-----	-----	-----	-----	-----	-----	-----
1	EXT1	V3	4:09	128	2	125
2	EXT3	V2	4:09	125	-	-
3	EXT4	V2	static	unknown	-	-

IGMP Mrouter information includes:

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

/info/13/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.
For example, once it receives a startup event, it transitions to master if its priority is 255, (the IP address owner), or transitions to backup if it is not the IP address owner.
- Server status. The `server` state identifies virtual routers.
- 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/qos

Quality of Service Information

```
[QoS Menu]
8021p      - Show QoS 802.1p information
```

Table 4-31 QoS Menu Options (/info/qos)

Command Syntax and Usage

8021p

Displays the 802.1p Information Menu. For details, see [page 114](#).

/info/qos/8021p

802.1p Information

```
Current priority to COS queue information:
```

```
Priority  COSq  Weight
```

```
-----  -
```

0	0	1
1	0	1
2	0	1
3	0	1
4	1	2
5	1	2
6	1	2
7	1	2

```
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 4-32 802.1p 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 4-33 802.1p 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/acl
Access Control List Information

```
Current ACL information:
-----
Filter 2 profile:
  Ethernet
    - VID      : 2/0xffff
  No ACL groups configured.
```

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

Table 4-34 ACL Parameter Descriptions

Parameter	Description
Filter x profile	Indicates the ACL number.
Actions	Displays the configured action for the ACL.

/info/link

Link Status Information

Alias	Port	Speed	Duplex	Flow Ctrl		Link
----	-----	-----	-----	--TX--	--RX--	-----
INT1	1	1000	full	yes	yes	up
INT2	2	1000	full	yes	yes	up
INT3	3	1000	full	yes	yes	up
INT4	4	1000	full	yes	yes	up
INT5	5	1000	full	yes	yes	down
INT6	6	1000	full	yes	yes	up
INT7	7	1000	full	yes	yes	up
INT8	8	1000	full	yes	yes	up
INT9	9	1000	full	yes	yes	up
INT10	10	1000	full	yes	yes	up
INT11	11	1000	full	yes	yes	up
INT12	12	1000	full	yes	yes	up
INT13	13	1000	full	yes	yes	up
INT14	14	1000	full	yes	yes	up
MGT1	15	100	full	yes	yes	up
MGT2	16	100	full	yes	yes	up
EXT1	17	1000	any	yes	yes	up
EXT2	18	1000	any	yes	yes	up
EXT3	19	1000	any	yes	yes	up
EXT4	20	1000	any	yes	yes	up
EXT5	21	1000	any	yes	yes	up
EXT6	22	1000	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 and number
- Port speed (10, 100, 1000, or any)
- Duplex mode (half, full, or any)
- Flow control for transmit and receive (no or yes)
- Link status (up, down, or disabled)

/info/port

Port Information

Alias	Port	Tag	Fast	Lrn	Fld	PVID	NAME	VLAN(s)
INT1	1	y	n	e	e	1	INT1	1 4095
INT2	2	y	n	e	e	1	INT2	1 4095
INT3	3	y	n	e	e	1	INT3	1 4095
INT4	4	y	n	e	e	1	INT4	1 4095
INT5	5	y	n	e	e	1	INT5	1 4095
INT6	6	y	n	e	e	1	INT6	1 4095
INT7	7	y	n	e	e	1	INT7	1 4095
INT8	8	y	n	e	e	1	INT8	1 4095
INT9	9	y	n	e	e	1	INT9	1 4095
INT10	10	y	n	e	e	1	INT10	1 4095
INT11	11	y	n	e	e	1	INT11	1 4095
INT12	12	y	n	e	e	1	INT12	1 4095
INT13	13	y	n	e	e	1	INT13	1 4095
INT14	14	y	n	e	e	1	INT14	1 4095
MGT1	15	y	n	e	e	4095	*MGT1	4095
MGT2	16	y	n	e	e	4095	*MGT2	4095
EXT1	17	n	n	e	e	1	EXT1	1
EXT2	18	n	n	e	e	1	EXT2	1
EXT3	19	n	n	e	e	1	EXT3	1
EXT4	20	n	n	e	e	1	EXT4	1
EXT5	21	n	n	e	e	1	EXT5	1
EXT6	22	n	n	e	e	1	EXT6	1

* = PVID is tagged.

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

Port information includes:

- Port alias and number
- Whether the port uses VLAN tagging or not (y or n)
- Whether the port is configured for Port Fast Forwarding (**F**ast)
- Whether the port is enabled for FDB Learning (**L**rn)
- Whether the port is enabled for flooding of unknown destination MACs (**F**ld)
- Port VLAN ID (**P**VID)
- Port name
- VLAN membership

/info/transcvr

Fiber Port Transceiver Status

Port	Device	TX-Enable	RX-Signal	TX-Fault
-----	-----	-----	-----	-----
17 - EXT1	FI-SFP	enabled	LOST	none
18 - EXT2	FI-SFP	enabled	LOST	none
19 - EXT3	FI-SFP	enabled	LOST	none
20 - EXT4	FI-SFP	enabled	LOST	none
21 - EXT5	FI-SFP	enabled	LOST	none
22 - EXT6	FI-SFP	enabled	LOST	none

This command displays the status of the Small Form Pluggable (SFP) transceiver 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
clrports  - Clear stats for all ports
l2        - Layer 2 Stats Menu
l3        - Layer 3 Stats Menu
mp        - MP-specific Stats Menu
acl       - ACL Stats Menu
snmp      - Show SNMP stats
ntp       - Show NTP stats
clrmp     - Clear all MP related stats
dump      - Dump all stats
```

The information provided by each menu option is briefly described in [Table 5-1](#), with pointers to detailed information.

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 123](#).

clrports

Clears statistics counters for all ports.

12

Displays the Layer 2 Stats Menu. To view menu options, see [page 135](#).

13

Displays the Layer 3 Stats Menu. To view menu options, see [page 137](#).

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 157](#).

acl

Displays ACL Statistics menu. To view menu options, see [page 161](#).

snmp

Displays SNMP statistics. See [page 163](#) for sample output.

ntp [clear]

Displays Network Time Protocol (NTP) Statistics. See [page 167](#) for a sample output and a description of NTP Statistics.

Use the following command to clear all NTP statistics: `ntp clear`

clrmp

Clears all management processor 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 168](#).

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

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 125](#) for sample output.

brg

Displays bridging ("dot1") statistics for the port. See [page 127](#) for sample output.

ether

Displays Ethernet ("dot3") statistics for the port. See [page 129](#) for sample output.

if

Displays interface statistics for the port. See [page 132](#) for sample output.

ip

Displays IP statistics for the port. See [page 134](#) for sample output.

link

Displays link statistics for the port. See [page 134](#) 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
eapolLogoff-FramesRx	Total number of EAPOL Logoff frames received
eapolRespId-FramesRx	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
invalidEapol-FramesRx	Total number of invalid EAPOL frames received
eapLengthError-FramesRx	Total number of EAP length error frames received
lastEapolFrameVer-sion	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
authEntersConnect- ing	Total number of times that the state machine transitions to the CONNECTING state from any other state.
authEapLogoffsWhi- leConnecting	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
authEntersAuthen- ticipating	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.

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

Statistics	Description
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.
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.

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

Statistics	Description
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
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.

Table 5-5 Bridging Statistics of a Port (/stats/port/brg)

Statistics	Description
dot1TpLearnedEntry Discards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
dot1StpPortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.

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

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

```
Ethernet statistics for port INT1:
dot3StatsAlignmentErrors:                0
dot3StatsFCSErrors:                      0
dot3StatsSingleCollisionFrames:          0
dot3StatsMultipleCollisionFrames:        0
dot3StatsLateCollisions:                 0
dot3StatsExcessiveCollisions:            0
dot3StatsInternalMacTransmitErrors:      NA
dot3StatsFrameTooLongs:                  0
dot3StatsInternalMacReceiveErrors:       0
```

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

Statistics	Description
dot3StatsAlignmentErrors	<p>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>alignmentError</code> status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsFCSErrors	<p>A count of frames received on a particular interface that are an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check.</p> <p>The count represented by an instance of this object is incremented when the <code>frameCheckError</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>
dot3StatsSingleCollisionFrames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsMultipleCollisionFrame</code> object.</p>

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

Statistics	Description
dot3StatsMultipleCollisionFrames	<p>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</p> <p>A frame that is counted by an instance of this object is also counted by the corresponding instance of either the <code>ifOutUcastPkts</code>, <code>ifOutMulticastPkts</code>, or <code>ifOutBroadcastPkts</code>, and is not counted by the corresponding instance of the <code>dot3StatsSingleCollisionFrames</code> object.</p>
dot3StatsLateCollisions	<p>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.</p> <p>Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</p>
dot3StatsExcessiveCollisions	<p>A count of frames for which transmission on a particular interface fails due to excessive collisions.</p>
dot3StatsInternalMacTransmitErrors	<p>A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the <code>dot3StatsLateCollisions</code> object, the <code>dot3StatsExcessiveCollisions</code> object, or the <code>dot3StatsCarrierSenseErrors</code> object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.</p>
dot3StatsFrameTooLongs	<p>A count of frames received on a particular interface that exceed the maximum permitted frame size.</p> <p>The count represented by an instance of this object is incremented when the <code>frameTooLong</code> status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p>

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

Statistics	Description
dot3StatsInternal- MacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3Stats-AlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

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

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

Interface statistics for port EXT1:		
	ifHCIn Counters	ifHCOut Counters
Octets:	51697080313	51721056808
UcastPkts:	65356399	65385714
BroadcastPkts:	0	6516
MulticastPkts:	0	0
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
<code>ifInUnknownProtos</code>	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.
<code>ifOutOctets</code>	The total number of octets transmitted out of the interface, including framing characters.
<code>ifOutUcastPkts</code>	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.
<code>ifOutBroadcastPkts</code>	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of <code>ifOutBroadcastPkts</code> .
<code>ifOutMulticastPkts</code>	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of <code>ifOutMulticastPkts</code> .
<code>ifOutDiscards</code>	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.
<code>ifOutErrors</code>	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

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

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

```
GEA IP statistics for port INT1:
ipInReceives      :      0
ipInHeaderError:    0
ipInDiscards      :      0
```

Table 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.
ipInHeaderErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

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

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

```
Link statistics for port INT1:
linkStateChange:      1
```

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

Statistics	Description
linkStateChange	The total number of link state changes.

/stats/l2
Layer 2 Statistics

[Layer 2 Statistics Menu]

fdb

- Show FDB stats

lACP

- Show LACP stats

The Layer 2 statistics provided by each menu option are briefly described in [Table 5-10](#), with pointers to detailed information.

Table 5-10 Layer 2 Statistics Menu Options (/stats/l2)

Command Syntax and Usage

fdb [clear]

Displays FDB statistics. See [page 135](#) for sample output.
Use the following command to clear all FDB statistics: fdb clear

lACP <port alias or number> [clear]

Displays Link Aggregation Control Protocol (LACP) statistics. See [page 136](#) for sample output.
Use the following command to clear all LACP statistics: lACP clear

/stats/l2/fdb [clear]
FDB Statistics

FDB statistics:

current:

83

hiwat:

855

This menu option enables you to display statistics regarding the use of the forwarding database, including the number of new entries, finds, and unsuccessful searches. Use the following command to clear all FDB statistics: fdb clear

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.

/stats/12/lacp *<port alias or number>* **[clear]**

LACP Statistics

```

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

```

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

Table 5-12 LACP Statistics (/stats/lacp)

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

/stats/l3

Layer 3 Statistics

```
[Layer 3 Statistics Menu]
geal3      - GEA Layer 3 Stats Menu
ip         - Show IP stats
route      - Show route stats
arp        - Show ARP stats
dns        - Show DNS stats
icmp       - Show ICMP stats
tcp        - Show TCP stats
udp        - Show UDP stats
igmp       - Show IGMP stats
ospf       - OSPF stats
vrrp       - Show VRRP stats
clrvrrp    - Clear VRRP stats
rip        - Show RIP stats
igmpgrps   - Total number of IGMP groups
ipmcgrps   - Total number of IPMC groups
clrigmp    - Clear IGMP stats
ipclear    - Clear IP stats
ripclear   - Clear RIP stats
ospfclear  - Clear all OSPF stats
dump       - Dump layer 3 stats
```

The Layer 3 statistics provided by each menu option are briefly described in [Table 5-13](#), with pointers to detailed information.

Table 5-13 Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage

geal3

Displays the Gigabit Ethernet Aggregators (GEA) statistics menu. GEA statistics are used by service and support personnel.

ip

Displays IP statistics. See [page 140](#) for sample output.

route [clear]

Displays route statistics. See [page 142](#) for sample output.

Use the following command to clear all route statistics: `route clear`

arp

Displays Address Resolution Protocol (ARP) statistics. See [page 142](#) for sample output.

Table 5-13 Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage

dns [clear]

Displays Domain Name System (DNS) statistics. See [page 143](#) for sample output.

Use the following command to clear all DNS statistics: `dns clear`

icmp [clear]

Displays ICMP statistics. See [page 143](#) for sample output.

Use the following command to clear all ICMP statistics: `icmp clear`

tcp [clear]

Displays TCP statistics. See [page 146](#) for sample output.

Use the following command to clear all TCP statistics: `tcp clear`

udp [clear]

Displays UDP statistics. See [page 148](#) for sample output.

Use the following command to clear all UDP statistics: `udp clear`

igmp

Displays IGMP statistics. See [page 149](#) for sample output.

ospf

Displays OSPF statistics. See [page 150](#) 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 155](#) for sample output.

clrvrrp

Clears VRRP statistics.

rip

Displays Routing Information Protocol (RIP) statistics. See [page 156](#) for sample output.

igmpgrps

Displays the total number of IGMP groups that are registered on the switch.

ipmcgrps

Displays the total number of current IP multicast groups that are registered on the switch.

clrigmp

Clears IGMP statistics.

Table 5-13 Layer 3 Statistics Menu Options (/stats/l3)

Command Syntax and Usage

ipclear

Clears IP statistics. Use this command with caution as it will delete all the IP statistics.

ripclear

Clears Routing Information Protocol (RIP) statistics.

ospfclear

Clears Open Shortest Path First (OSPF) statistics.

dump

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

/stats/l3/ip 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 5-14 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.
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.

Table 5-14 IP Statistics (stats/l3/ip)

Statistics	Description
ipInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams, which meet this <i>no-route</i> criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
ipReasmReqds	The number of IP fragments received which needed to be reassembled at this entity (the switch).
ipReasmOKs	The number of IP datagrams successfully re- assembled.
ipReasmFails	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, and so forth). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
ipFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their Don't Fragment flag was set.
ipFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).
ipRoutingDiscards	The number of routing entries, which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.

Table 5-14 IP Statistics (stats/l3/ip)

Statistics	Description
ipReasmTimeout	The maximum number of seconds, which received fragments are held while they are awaiting reassembly at this entity (the switch).

/stats/l3/route [clear] Route Statistics

```
Route statistics:
ipRoutesCur:          11  ipRoutesHighWater:      11
ipRoutesMax:          2048
```

Table 5-15 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.

/stats/l3/arp ARP statistics

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

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

Table 5-16 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.

/stats/l3/dns [clear]

DNS Statistics

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

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

Table 5-17 DNS Statistics (/stats/dns)

Statistics	Description
dnsInRequests	The total number of DNS request packets that have been received.
dnsOutRequests	The total number of DNS response packets that have been transmitted.
dnsBadRequests	The total number of DNS request packets received that were dropped.

/stats/l3/icmp [clear]

ICMP Statistics

```
ICMP statistics:
icmpInMsgs:      245802  icmpInErrors:      1393
icmpInDestUnreaches:  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  icmpOutDestUnreaches: 15
icmpOutTimeExcds:   0  icmpOutParmProbs:   0
icmpOutSrcQuenchs:  0  icmpOutRedirects:   0
icmpOutEchos:       253777  icmpOutEchoReps:   18
icmpOutTimestamps:  0  icmpOutTimestampReps: 0
icmpOutAddrMasks:   0  icmpOutAddrMaskReps: 0
```

Table 5-18 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).

Table 5-18 ICMP Statistics (/stats/l3/icmp)

Statistics	Description
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.
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.

Table 5-18 ICMP Statistics (/stats/l3/icmp)

Statistics	Description
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/tcp [clear]

TCP Statistics

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

Table 5-19 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 5-19 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 [clear]
UDP Statistics

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

Table 5-20 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 <VLAN number> **IGMP Statistics**

IGMP Snoop vlan 2 statistics:			

rxIgmpValidPkts:	0	rxIgmpInvalidPkts:	0
rxIgmpGenQueries:	0	rxIgmpGrpSpecificQueries:	0
rxIgmpGroupSrcSpecificQueries:	0		
rxIgmpLeaves:	0	rxIgmpReports:	0
txIgmpReports:	0	txIgmpGrpSpecificQueries:	0
txIgmpLeaves:	0	rxIgmpV3CurrentStateRecords:	0
rxIgmpV3SourceListChangeRecords:	0	rxIgmpV3FilterChangeRecords:	0

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

Table 5-21 IGMP Statistics (/stats/l3/igmp)

Statistic	Description
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpGroupSrcSpecificQueries	Total number of Group Source-Specific Queries (GSSQ) received
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
rxIgmpV3CurrentStateRecords	Total number of Current State records received
rxIgmpV3SourceListChangeRecords	Total number of Source List Change records received.
rxIgmpV3FilterChangeRecords	Total number of Filter Change records received.

/stats/l3/ospf

OSPF Statistics

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

Table 5-22 OSPF Statistics Menu (/stats/l3/ospf)

Command Syntax and Usage

general

Displays global statistics. See [page 151](#) for sample output.

aindex

Displays area statistics.

if

Displays interface statistics.

/stats/13/ospf/general

OSPF Global Statistics

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

OSPF stats			

Rx/Tx Stats:	Rx	Tx	
	-----	-----	
Pkts	0	0	
hello	23	518	
database	4	12	
ls requests	3	1	
ls acks	7	7	
ls updates	9	7	
Nbr change stats:		Intf change Stats:	
hello	2	hello	4
start	0	down	2
n2way	2	loop	0
adjoint ok	2	unloop	0
negotiation done	2	wait timer	2
exchange done	2	backup	0
bad requests	0	nbr change	5
bad sequence	0		
loading done	2		
nlway	0		
rst_ad	0		
down	1		
Timers kickoff			
hello	514		
retransmit	1028		
lsa lock	0		
lsa ack	0		
dbage	0		
summary	0		
ase export	0		

Table 5-23 OSPF General Statistics (stats/l3/ospf/general)

Statistics	Description
Rx/Tx Stats:	
Rx Pkts	The sum total of all OSPF packets received on all OSPF areas and interfaces.
Tx Pkts	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
Rx Hello	The sum total of all Hello packets received on all OSPF areas and interfaces.
Tx Hello	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
Rx Database	The sum total of all Database Description packets received on all OSPF areas and interfaces.
Tx Database	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
Rx ls Requests	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
Tx ls Requests	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
Rx ls Acks	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
Tx ls Acks	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
Rx ls Updates	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx ls Updates	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.

Table 5-23 OSPF General Statistics (stats/l3/ospf/general) (Continued)

Statistics	Description
Nbr Change Stats:	
hello	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Start	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds.) across all OSPF areas and interfaces.
n2way	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
adjoint ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
negotiation done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
exchange done	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
bad requests	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.
bad sequence	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> a) Has an unexpected DD sequence number b) Unexpectedly has the init bit set c) Has an options field differing from the last Options field received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
nlway	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation.) across all OSPF areas and interfaces.

Table 5-23 OSPF General Statistics (stats/l3/ospf/general) (Continued)

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

/stats/l3/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.

The statistics for the VRRP LAN are displayed:

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

Table 5-24 VRRP Statistics (/stats/l3/vrrp)

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

/stats/13/rip

Routing Information Protocol Statistics

```
RIP ALL STATS INFORMATION:
  RIP packets received = 12
  RIP packets sent     = 75
  RIP request received = 0
  RIP response received = 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

Table 5-25 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 158 .
tcb	Displays all TCP control blocks that are in use. To view a sample output and a description of the stats, see page 159 .
ucb	Displays all UDP control blocks that are in use. To view a sample output, see page 159 .
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 160 .

/stats/mp/pkt

MP Packet Statistics

```

Packet counts:
allocs:          1722684      frees:          1722684
mediums:         0           mediums hi-watermark: 4
jumbos:         0           jumbos hi-watermark: 0
smalls:         0           smalls hi-watermark: 8
failures:        0

```

Table 5-26 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.
mediums hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with more than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with more than 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.
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.
failures	Total number of packet allocation failures 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 5-27 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/cpu
CPU Statistics

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

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

Table 5-28 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	- Display ACL stats
meter	- Display ACL metering stats
dump	- Display all available ACL stats
clracl	- Clear ACL stats
clrmeter	- Clear ACL metering stats

ACL statistics are described in the following table.

Table 5-29 ACL 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 161](#).

meter <1-127>

Displays statistics for a specific ACL Meter. For details, see [page 162](#).

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 ACL statistics.

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 ACL meter statistics.

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

/stats/snmp

SNMP Statistics

NOTE – Use the following command to reset the SNMP counter to zero: `snmp clear`

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

Table 5-30 SNMP Statistics (/stats/snmp)

Statistics	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadCommunityNames	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).
snmpInBadCommunityUses	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Table 5-30 SNMP Statistics (/stats/snmp)

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

Table 5-30 SNMP Statistics (/stats/snmp)

Statistics	Description
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 <i>too big</i> .
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is <i>noSuchName</i> .
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is <i>badValue</i> .
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 <i>genErr</i> .
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 5-30 SNMP Statistics (/stats/snmp)

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

`/stats/ntp [clear]`

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.

Use the following command to clear all NTP statistics: `ntp clear`

```
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 17, 2007
  Current system time: 18:55:49 Tue Jul 17, 2007
```

Table 5-31 NTP Statistics Parameters (/stats/ntp)

Field	Description
Primary Server	<p>Requests Sent: The total number of NTP requests the switch sent to the primary NTP server to synchronize time.</p> <p>Responses Received: The total number of NTP responses received from the primary NTP server.</p> <p>Updates: The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.</p>
Secondary Server	<p>Requests Sent: The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.</p> <p>Responses Received: The total number of NTP responses received from the secondary NTP server.</p> <p>Updates: The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.</p>

Table 5-31 NTP Statistics Parameters (/stats/ntp)

Field	Description
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 <code>/stats/ntp</code> was issued.

`/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
  pmirr    - Port Mirroring Menu
  l2       - Layer 2 Menu
  l3       - Layer 3 Menu
  qos      - QOS Menu
  acl      - Access Control List Menu
  setup    - Step by step configuration set up
  dump     - Dump current configuration to script file
  ptcfg    - Backup current configuration to FTP/TFTP server
  gtcfg    - Restore current configuration from FTP/TFTP server
  cur      - Display current configuration
```

Each configuration option is briefly described in [Table 6-1](#), with pointers to detailed menu commands.

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage

sys

Displays the System Configuration Menu. To view menu options, see [page 174](#).

port <port alias or number>

Displays the Port Configuration Menu. To view menu options, see [page 207](#).

pmirr

Displays the Mirroring Configuration Menu. To view menu options, see [page 319](#).

l2

Displays the Layer 2 Configuration Menu. To view menu options, see [page 216](#).

l3

Displays the Layer 3 Configuration Menu. To view menu options, see [page 252](#).

qos

Displays the Quality of Service Configuration Menu. To view menu options, see [page 308](#).

acl

Displays the ACL Configuration Menu. To view menu options, see [page 311](#).

setup

Step-by-step configuration set-up of the switch. For details, see [page 321](#).

Table 6-1 Configuration Menu Options (/cfg)

Command Syntax and Usage

dump

Dumps current configuration to a script file. For details, see [page 321](#).

ptcfg *<host name or IP address of TFTP server> <filename on host>*

Backs up current configuration to TFTP server. For details, see [page 322](#).

gtcfg *<host name or IP address of TFTP server> <filename on host>*

Restores current configuration from TFTP server. For details, see [page 322](#).

cur

Displays current configuration parameters.

Viewing, Applying, and Saving Changes

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

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

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

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

Viewing Pending Changes

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

NOTE – The **diff** command is a global command. Therefore, you can enter **diff** at any prompt in the CLI.

Applying Pending Changes

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

```
# apply
```

NOTE – The **apply** command is a global command. Therefore, you can enter **apply** at any prompt in the administrative interface.

Saving the Configuration

In addition to applying the configuration changes, you can save them to flash memory on the 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 340](#).

/cfg/sys

System Configuration

[System Menu]	
syslog	- Syslog Menu
sshd	- SSH Server Menu
radius	- RADIUS Authentication Menu
tacacs+	- TACACS+ Authentication Menu
ldap	- LDAP Authentication Menu
ntp	- NTP Server Menu
ssnmp	- System SNMP Menu
access	- System Access Menu
date	- Set system date
time	- Set system time
timezone	- Set system timezone (daylight savings)
olddst	- Set system DST for US
dlight	- Set system daylight savings
idle	- Set timeout for idle CLI sessions
notice	- Set login notice
e2e	- Enable/disable end-to-end flow control mode
hgibp	- Enable/disable higig IBP
bannr	- Set login banner
hprompt	- Enable/disable display hostname (sysName) in CLI prompt
reminder	- Enable/disable Reminders
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 177](#).

sshd

Displays the SSH Server Menu. To view menu options, see [page 178](#).

radius

Displays the RADIUS Authentication Menu. To view menu options, see [page 179](#).

tacacs+

Displays the TACACS+ Authentication Menu. To view menu options, see [page 181](#).

ldap

Displays the LDAP Authentication Menu. To view menu options, see [page 184](#).

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

Command Syntax and Usage

ntp

Displays the Network Time Protocol (NTP) Server Menu.

To view menu options, see [page 186](#).

ssnmp

Displays the System SNMP Menu. To view menu options, see [page 187](#).

access

Displays the System Access Menu. To view menu options, see [page 200](#).

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.

olddst enable|disable

Enables or disables use of the Daylight Saving Time (DST) rules in effect prior to the year 2007.

The default value is **disabled**.

dlight enable|disable

Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock.

The default value is **enabled**.

idle *<idle timeout in minutes>*

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.

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

Command Syntax and Usage

e2e enable|disable

Enables or disables End-to-End flow control mode. The default value is **enabled**. If you change the flow-control mode, you must apply and save the changes, then reboot the switch before the change takes effect.

The GbE switch module has two switching chips connected by an internal high-capacity link (Higig). Over subscription of traffic across the Higig link is handled by one of the following flow control modes:

- End-to-End (E2E) Flow Control
- Ingress Back Pressure (IBP) across the Higig link

One of the modes should be enabled, and the other mode disabled. E2E flow control works best for most applications. E2E provides a higher throughput and better overall switch performance, but does not provide lossless flow control.

hgibp enable|disable

Enables or disables Higig Ingress Back Pressure (IBP) flow control mode. The default value is **disabled**. If you change the flow-control mode, you must apply and save the changes, then reboot the switch before the change takes effect.

The GbE switch module has two switching chips connected by an internal high-capacity link (Higig). Over subscription of traffic across the Higig link is handled by one of the following flow control modes:

- End-to-End (E2E) Flow Control
- Ingress Back Pressure (IBP) across the Higig link

One of the modes should be enabled, and the other mode disabled. Applications that cannot tolerate packet loss might require IBP across the Higig link. Higig IPB achieves lossless operation, but it might result in a lower throughput.

bannr <string, maximum 80 characters>

Configures a login banner of up to 80 characters. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `/info/sys` command.

hprompt disable|enable

Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).

reminder disable|enable

Enables or disables reminder messages in the CLI. The default value is **enabled**.

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 Host Log 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 severity levels.

sever2 <syslog host local severity (0-7)>

This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all severity levels.

facil <syslog host local facility (0-7)>

This option sets the facility level of the first syslog host displayed. The default is 0.

facil2 <syslog host local facility (0-7)>

This option sets the facility level of the second syslog host displayed. The default is 0.

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, stg, or servers), or enable/disable syslog on all available features.

cur

Displays the current syslog settings.

/cfg/sys/sshd

SSH Server Configuration

[SSHD Menu]	
interval	- 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 321](#)).

NOTE – Only the following commands are accessible through a serial connection:
ena, on, off, cur

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

Command Syntax and Usage

interval <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 Secure Shell 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
bckdoor - Enable/disable RADIUS backdoor for telnet/ssh/http/https
on - Turn RADIUS authentication ON
off - Turn RADIUS authentication OFF
cur - Display current RADIUS configuration
```

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

Command Syntax and Usage	
timeout	<i><RADIUS server timeout seconds (1-10)></i> Sets the amount of time, in seconds, before a RADIUS server authentication attempt is considered to have failed. The default is 3 seconds.
bckdoor	disable enable Enables or disables the RADIUS backdoor for telnet. The bckdoor command also applies to SSH/SCP connections and the Browser-Based Interface (BBI). The default setting 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

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 IP address of primary TACACS+ server
  secsrv   - Set IP address of secondary TACACS+ server
  secret   - Set secret for primary TACACS+ server
  secret2  - Set secret for secondary TACACS+ server
  port     - Set TACACS+ port number
  retries  - Set number of TACACS+ server retries
  timeout  - Set timeout value of TACACS+ server retries
  bckdoor  - Enable/disable TACACS+ backdoor for telnet/ssh/
             http/https
  secbd    - Enable/disable TACACS+ secure backdoor for telnet/
             ssh/http
  cmap     - Enable/disable TACACS+ new privilege level mapping
  passsch  - Enable/disable TACACS+ password change
  chpass_p - Set new password for primary server
  chpass_s - Set new password for secondary server
  cauth    - Enable/disable TACACS+ command authorization
  clog     - Enable/disable TACACS+ command logging
  on       - Enable TACACS+ authentication
  off      - Disable TACACS+ authentication
  cur      - Display current TACACS+ settings
```

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.

bckdoor **disable**|**enable**

Enables or disables the TACACS+ back door for Telnet, SSH/SCP, or HTTP/HTTPS.

Enabling this feature allows you to bypass the TACACS+ servers. It is recommended that you use Secure Backdoor to ensure the switch is secured, because Secure Backdoor disallows access through the back door when the TACACS+ servers are responding.

The default is disabled.

To obtain the TACACS+ backdoor password for your GbESM, contact your IBM Service and Support line.

secbd **enable**|**disable**

Enables or disables TACACS+ secure back door access through Telnet, SSH/SCP, or HTTP/HTTPS only when the TACACS+ servers are not responding.

This feature is recommended to permit access to the switch when the TACACS+ servers become unresponsive. If no back door is enabled, the only way to gain access when TACACS+ servers are unresponsive is to use the back door via the console port.

The default is disabled.

cmap **enable**|**disable**

Enables or disables TACACS+ privilege-level mapping.

The default value is disabled.

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

Command Syntax and Usage	
passch enable disable	Enables or disables TACACS+ password change. The default value is disabled.
chpass_p	Configures the password for the primary TACACS+ server. The CLI will prompt you for input.
chpass_s	Configures the password for the secondary TACACS+ server. The CLI will prompt you for input.
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/ldap

LDAP Server Configuration

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

```
[LDAP Server Menu]
prisrv    - Set IP address of primary LDAP server
secsrv    - Set IP address of secondary LDAP server
port      - Set LDAP port number
retries   - Set number of LDAP server retries
timeout   - Set timeout value of LDAP server retries
domain    - Set domain name
telnet    - Enable/disable LDAP backdoor for telnet/ssh/http
on        - Enable LDAP authentication
off       - Disable LDAP authentication
cur       - Display current LDAP settings
```

Table 6-7 LDAP Server Menu Options (/cfg/sys/ldap)

Command Syntax and Usage

prisrv <IP address>

Defines the primary LDAP server address.

secsrv <IP address>

Defines the secondary LDAP server address.

port <LDAP port configure, default 389>

Enter the number of the TCP port to be configured, between 1 - 65000. The default is 389.

retries <LDAP server retries, 1-3>

Sets the number of failed authentication requests before switching to a different LDAP server. The default is 3 requests.

timeout <LDAP server timeout seconds, 4-15>

Sets the amount of time, in seconds, before a LDAP server authentication attempt is considered to have failed. The default is 5 seconds.

domain <domain name (1-128 characters)> | none

Sets the domain name for the LDAP server. Enter the full path for your organization. For example:
ou=people,dc=mydomain,dc=com

Table 6-7 LDAP Server Menu Options (/cfg/sys/ldap)

Command Syntax and Usage	
telnet disable enable	Enables or disables the LDAP back door for telnet. The <code>telnet</code> command also applies to SSH/SCP connections, and the Browser-Based Interface (BBI). The default is <code>disabled</code> . To obtain the LDAP backdoor password for your GbESM, contact your IBM Service and Support line.
on	Enables the LDAP server.
off	Disables the LDAP server. This is the default setting.
cur	Displays current LDAP configuration parameters.

/cfg/sys/ntp

NTP Server Configuration

```
[NTP Server Menu]
  prisrv  - Set primary NTP server address
  secsrv  - Set secondary NTP server address
  intrval - Set NTP server resync interval
  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 6-8 NTP 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.

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
trsrc     - Set SNMP trap source interface
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 6-9 System SNMP Menu Options (/cfg/sys/ssnmp)**Command Syntax and Usage****snmpv3**

Displays SNMPv3 menu. To view menu options, see [page 189](#).

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*.

trsrc *<1-128>*

Configures the source interface for SNMP traps.

timeout *<1-30>*

Set the timeout value for the SNMP state machine, in minutes.

auth **disable** | **enable**

Enables or disables the use of the system authentication trap facility. The default setting is disabled.

linkt *<port>* [**disable** | **enable**]

Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.

cur

Displays the current SNMP configuration.

/cfg/sys/ssnmp/snmpv3

SNMPv3 Configuration

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
vlv2	- Enable/disable V1/V2 access
cur	- Display current SNMPv3 configuration

Table 6-10 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 191](#).

view <vacmViewTreeFamily number [1-128]>

This command allows you to create different MIB views. To view menu options, see [page 192](#).

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 193](#).

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 195](#).

Table 6-10 SNMPv3 Configuration Menu Options (/cfg/sys/ssnmp/snmpv3)

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 196](#).

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 197](#).

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 198](#).

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 199](#).

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

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 6-11 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 6-11 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/view
SNMPv3 View Configuration

```
[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 6-12 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/access

View-based Access Control Model Configuration

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

```
[SNMPv3 vacmAccess 1 Menu]
  name      - Set group name
  model     - Set security model
  level     - Set minimum level of security
  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 6-13 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.

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.

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.

Table 6-13 View-based Access Control Model Menu Options (/cfg/sys/ssnmp/snmpv3/access)

Command Syntax and Usage

del

Deletes the View-based Access Control entry.

cur

Displays the View-based Access Control configuration.

/cfg/sys/ssnmp/snmpv3/group
SNMPv3 Group Configuration

[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 6-14 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 191](#).

gname *<32 character name>*

The name for the access group as defined in /cfg/sys/ssnmp/snmpv3/access/name on [page 193](#).

del

Deletes the vacmSecurityToGroup entry.

cur

Displays the current vacmSecurityToGroup configuration.

/cfg/sys/ssnmp/snmpv3/comm

SNMPv3 Community Table Configuration

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 6-15 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

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

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 6-16 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 198 .
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

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 6-17 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 191](#)) on whose behalf the SNMP messages are generated using this entry.

level **noAuthNoPriv** | **authNoPriv** | **authPriv**

Allows you to select the level of security to be used when generating the SNMP messages using this entry. The level **noAuthNoPriv** means that the SNMP message will be sent without authentication and without using a privacy protocol. The level **authNoPriv** means that the SNMP message will be sent with authentication but without using a privacy protocol. The **authPriv** means that the SNMP message will be sent both with authentication and using a privacy protocol.

del

Deletes the targetParamsTable entry.

cur

Displays the current targetParamsTable configuration.

/cfg/sys/ssnmp/snmpv3/notify
SNMPv3 Notify Table Configuration

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 6-18 Notify Table Menu Options (/cfg/sys/ssnmp/snmpv3/notify)

Command Syntax and Usage

name	<i><32 character name></i> Defines a locally arbitrary but unique identifier associated with this SNMP notify entry.
tag	<i><list of tag string, max 255 characters></i> 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 Configuration

```
[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
  userbbi   - Enable/disable user configuration from BBI
  tsbbi     - Enable/disable telnet/ssh configuration from BBI
  tnet      - Enable/disable Telnet access
  tnport    - Set Telnet server port number
  tport     - Set the TFTP port for the system
  cur       - Display current system access configuration
```

Table 6-19 System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage

mgmt

Displays the Management Configuration Menu. To view menu options, see [page 202](#).

user

Displays the User Access Control Menu. To view menu options, see [page 203](#).

http disable|enable

Enables or disables HTTP (Web) access to the Browser-Based Interface. It is enabled by default.

https

Displays the HTTPS Menu. To view menu options, see [page 206](#).

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.

userbbi enable|disable

Enables or disables user configuration access through the Browser-Based Interface (BBI).

tsbbi enable|disable

Enables or disables Telnet/SSH configuration access through the Browser-Based Interface (BBI).

tnet enable|disable

Enables or disables Telnet access. This command is enabled by default. You see this command only if you are connected to the switch through a serial connection.

Table 6-19 System Access Menu Options (/cfg/sys/access)

Command Syntax and Usage	
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.
tpport <TFTP port number (1-65535)>	Sets the TFTP port for the switch. The default is port 69.
cur	Displays the current system access parameters.

`/cfg/sys/access/mgmt` Management Networks Configuration

[Management Networks Menu]	
<code>add</code>	- Add mgmt network definition
<code>rem</code>	- Remove mgmt network definition
<code>cur</code>	- Display current mgmt network definitions
<code>clear</code>	- Clear current mgmt network definitions

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

Table 6-20 Management Network Menu Options (`/cfg/sys/access/mgmt`)

Command Syntax and Usage	
add <i><mgmt network address> <mgmt network mask></i>	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 <i><mgmt network address> <mgmt network mask></i>	Removes a defined network, which consists of a management network address and a management network mask address.
cur	Displays the current configuration.
clear	Clears the current management network definitions.

/cfg/sys/access/user

User Access Control Configuration

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

NOTE – User passwords can be a maximum of 128 characters.

Table 6-21 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 204](#).

eject user|oper|admin <user name>

Ejects the specified user from the GbESM.

usrpw <1-128 characters>

Sets the user (user) password. The user has no direct responsibility for switch management. He or she can view switch status information and statistics, but cannot make any configuration changes.

opw <1-128 characters>

Sets the operator (oper) password. The operator manages all functions of the switch. He or she can view all switch information and statistics and can reset ports, except the management ports.

admpw <1-128 characters>

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.

strongpw

Displays the Strong User Password Menu. To view menu options, see [page 205](#).

cur

Displays the current user status.

/cfg/sys/access/user/uid <1-10>

System User ID Configuration

[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 6-22 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 <1-8 characters>	Defines the user name of maximum eight characters.
pswd <1-128 characters>	Sets the user password.
ena	Enables the user ID.
dis	Disables the user ID.
del	Deletes the user ID.
cur	Displays the current user ID configuration.

/cfg/sys/access/user/strongpw
Strong Password Configuration

[Strong Pwd Menu]	
ena	- Enable usage of strong passwords
dis	- Disable usage of strong passwords
expiry	- Set password validity
warning	- Set warning days before pswd expiry
faillog	- Set number of failed logins for security notification
cur	- Display current strong password configuration

Table 6-23 Strong Password Menu Options (/cfg/sys/access/user/strongpw)

Command Syntax and Usage

ena	Enables Strong Password requirement.
dis	Disables Strong Password requirement.
expiry <1-365>	Configures the number of days allowed before the password must be changed.
warning <1-365>	Configures the number of days before password expiration, that a warning is issued to users.
faillog <1-255>	Configures the number of failed login attempts allowed before a security notification is logged.
cur	Displays the current Strong Password configuration.

/cfg/sys/access/https

HTTPS Access Configuration

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

Table 6-24 HTTPS Access Configuration Menu Options (/cfg/sys/access/https)

Command Syntax and Usage

access ena|dis

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

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) []: Blade
- Organizational Unit Name (for example, section) []: Alteon
- Common Name (for example, user's name) []: Mr Smith
- Email (for example, email address) []: info@bladenetwork.net

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
  802lppri - 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
  tagpvid  - Enable/disable tagging on pvid
  fastfwd  - Enable/disable Port Fast Forwarding mode
  ena      - Enable port
  dis      - Disable port
  cur      - Display current port configuration
```

Use the Port Configuration menu to configure settings for individual switch ports, except the management port (MGT). This command is enabled by default.

Table 6-25 Port Configuration Menu (/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 209](#).

aclqos

Displays the ACL Quality of Service Menu. To view menu options, see [page 210](#).

802lppri <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 6-25 Port Configuration Menu (/cfg/port)

Command Syntax and Usage	
tagpvid disable enable	Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is disabled for INT and EXT ports, and enabled for MGT ports.
fastfwd disable enable	Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state. This feature permits the GbESM to interoperate well within Rapid Spanning Tree networks.
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 210.)
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.

Link menu options are described in [Table 6-26](#) and appear on the gig port configuration menu for the GbE Switch Module. Use this menu to set port parameters such as speed, flow control, and negotiation mode for the port link.

Table 6-26 Port Link Configuration Menu Options (/cfg/port/gig)

Command Syntax and Usage

speed 10 | 100 | 1000 | any

Sets the link speed. Some options are not valid on all ports. The choices include:

- 10 Mbps
- 100 Mbps
- 1000 Mbps
- “Auto,” for auto negotiation

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

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 324](#) for other operations-level commands.

/cfg/port <port alias or number> aclqos Port ACL Configuration

```
[Port INT2 ACL Menu]
meter      - ACL Metering Configuration Menu
re-mark    - ACL Re-mark Configuration Menu
add        - Add ACL, ACL block or ACL group to this port
rem        - Remove ACL, ACL block or ACL group from this port
cur        - Display current ACLs for this port
```

Table 6-27 Port ACL Menu Options (/cfg/port/aclqos)

Command Syntax and Usage	
meter <meter number, 1-127>	Displays the Metering Menu. To view menu options, see page 211 .
re-mark <re-mark number, 1-127>	Displays the Re-Mark Menu. To view menu options, see page 212 .
add acl blk grp <1-4096>	Adds the specified ACL, ACL Block, or ACL Group to the port. You can add multiple ACL Groups to a port, but the total number of precedence levels allowed is eight.
rem acl blk grp <1-4096>	Removes the specified ACL, ACL Block, or ACL Group 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 6-28 ACL 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 <ACL re-mark number>
Re-Mark Menu**

[Re-mark 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 6-29 ACL 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 213 .
outprof	Displays the Re-Mark Out-of-Profile Menu. To view menu options, see page 214 .
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 re-mark number> /inprof**
Re-Marking In-Profile Menu

[Re-marking - In Profile Menu]	
uplp	- Set Update User Priority Menu
updscp	- Set the update DSCP
reset	- Reset update DSCP settings
cur	- Display current settings

Table 6-30 ACL Re-Mark In-Profile Options (/cfg/port/aclqos/re-mark/inprof)

Command Syntax and Usage

uplp	Displays the Re-Mark In-Profile Update User Priority Menu. To view menu options, see page 215 .
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 <ACL re-mark number> /inprof/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 6-31 ACL Re-mark 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 re-mark number> /outprof**
Re-Marking Out-of-Profile Menu

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

Table 6-32 ACL Re-mark Out-of-Profile Options (/cfg/port/aclqos/re-mark/
outprof)

Command Syntax and Usage

- updsdp** <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/12

Layer 2 Configuration

```
[Layer 2 Menu]
  8021x      - 802.1X Menu
  mrst       - Multiple Spanning Tree/Rapid Spanning Tree Menu
  stg        - Spanning Tree Menu
  fdb        - FDB
  trunk      - Trunk Group Menu
  thash      - IP Trunk Hash Menu
  lacp       - Link Aggregation Control Protocol Menu
  failover   - Failover Menu
  vlan       - VLAN Menu
  pvstcomp   - Enable/Disable PVST+ compatibility mode
  bpdugrd    - Enable/disable BPDU Guard
  macnotif   - Enable/disable MAC address notification
  upfast     - Enable/disable Uplink Fast
  update     - UplinkFast station update rate
  cur        - Display current layer 2 parameters
```

Table 6-33 Layer 2 Configuration Menu (/cfg/12)

Command Syntax and Usage

8021x

Displays the 802.1X Configuration Menu. To view menu options, see [page 218](#).

mrst

Displays the Rapid Spanning Tree/Multiple Spanning Tree Protocol Configuration Menu. To view menu options, see [page 224](#).

stg <group number [1-128]>

Displays the Spanning Tree Configuration Menu. To view menu options, see [page 230](#).

fdb

Displays the Forwarding Database (FDB) Menu. To view menu options, see [page 236](#).

trunk <trunk group number (1-13)>

Displays the Trunk Group Configuration Menu. To view menu options, see [page 238](#).

thash

Displays the IP Trunk Hash Menu. To view menu options, see [page 239](#).

lacp

Displays the Link Aggregation Control Protocol Menu. To view menu options, see [page 241](#).

failover

Displays the Failover Configuration Menu. To view menu options, see [page 243](#).

Table 6-33 Layer 2 Configuration Menu (/cfg/l2)

Command Syntax and Usage

vlan <VLAN number (1-4095)>Displays the VLAN Configuration Menu. To view menu options, see [page 246](#).

pvstcomp enable|disableEnables or disables VLAN tagging of spanning tree BPDUs. The default value is **enabled**.

bpdugrd enable|disable

Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled (/cfg/port x/fastfwd ena).

macnotif enable|disable

Enables or disables MAC Address Notification. With MAC Address Notification enabled, the switch generates a syslog message when a MAC address is added or removed from the MAC address table.

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 <10-200>

Configures the station update rate. The default value is 40.

curDisplays 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 6-34 802.1X Configuration Menu (`/cfg/l2/8021x`)

Command Syntax and Usage

global

Displays the global 802.1X Configuration Menu. To view menu options, see [page 219](#).

port *<port alias or number>*

Displays the 802.1X Port Menu. To view menu options, see [page 222](#).

ena

Globally enables 802.1X.

dis

Globally disables 802.1X.

cur

Displays current 802.1X parameters.

/cfg/l2/8021x/global

802.1X Global Configuration

```
[802.1X Global Configuration Menu]
  gvlan      - 802.1X Guest VLAN configuration menu
  mode       - Set access control mode
  qtperiod   - Set EAP-Request/Identity quiet time interval
  txperiod   - Set EAP-Request/Identity retransmission timeout
  suptmout   - Set EAP-Request retransmission timeout
  svrtmout   - Set server authentication request timeout
  maxreq     - Set max number of EAP-Request retransmissions
  raperiod   - Set reauthentication time interval
  reauth     - Set reauthentication status to on or off
  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 6-35 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)

Command Syntax and Usage

gvlan

Displays the 802.1X Guest VLAN Configuration Menu. To view menu options, see [page 221](#).

mode force-unauth|auto|force-auth

Sets the type of access control for all ports:

- **force-unauth** - the port is unauthorized unconditionally.
- **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- **force-auth** - the port is authorized unconditionally, allowing all traffic.

The default value is **force-auth**.

qtperiod <0-65535>

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

txperiod <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

suptmout <1-65535>

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

Table 6-35 802.1X Global Configuration Menu Options (/cfg/l2/8021x/global)

Command Syntax and Usage

svrtimeout <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/global/gvlan
802.1X Guest VLAN Configuration

[802.1X Guest VLAN Configuration Menu]	
vlan	- Set 8021.x Guest VLAN number
ena	- Enable 8021.xGuest VLAN
dis	- Disable 8021.x Guest VLAN
cur	- Display current Guest VLAN configuration

The 802.1X Guest VLAN menu allows you to configure a Guest VLAN for unauthenticated ports. The Guest VLAN provides limited access to switch functions.

Table 6-36 802.1X Guest VLAN Configuration Menu (/cfg/l2/8021x/global/gvlan)

Command Syntax and Usage

vlan <1-4094>	Configures the Guest VLAN number.
ena	Enables the 802.1X Guest VLAN.
dis	Disables the 802.1X Guest VLAN.
cur	Displays current 802.1X Guest VLAN parameters.

/cfg/l2/8021x/port *<alias or number>*

802.1X Port Configuration

```
[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 6-37 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

Command Syntax and Usage

mode **force-unauth|auto|force-auth**

Sets the type of access control for the port:

- **force-unauth** - the port is unauthorized unconditionally.
- **auto** - the port is unauthorized until it is successfully authorized by the RADIUS server.
- **force-auth** - the port is authorized unconditionally, allowing all traffic.

The default value is **force-auth**.

qtperiod *<0-65535>*

Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.

txperiod *<1-65535>*

Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.

suptmout *<1-65535>*

Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.

Table 6-37 802.1X Port Configuration Menu Options (/cfg/l2/8021x/port)

Command Syntax and Usage	
svrtimeout <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]	
<code>cist</code>	- Common and Internal Spanning Tree menu
<code>name</code>	- Set MST region name
<code>rev</code>	- Set revision level of this MST region
<code>maxhop</code>	- Set Maximum Hop Count for MST (4 - 60)
<code>mode</code>	- Spanning Tree Mode
<code>on</code>	- Globally turn Multiple Spanning Tree (MSTP/RSTP) ON
<code>off</code>	- Globally turn Multiple Spanning Tree (MSTP/RSTP) OFF
<code>cur</code>	- 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.

Up to 32 Spanning Tree Groups can be configured in **mstp** mode. MRST is turned off by default.

NOTE – When Multiple Spanning Tree is turned on, management VLANs are moved from Spanning Tree Group 128 to the Common Internal Spanning Tree (CIST). When Multiple Spanning Tree is turned off, management VLANs are moved back to Spanning Tree Group 128.

Table 6-38 MSTP/RSTP 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 226](#).

name *<1-32 characters>*

Configures a name for the MSTP region. All devices within a MSTP region must have the same region name.

rev *<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.

maxhop *<4-60>*

Configures the maximum number of bridge hops a packet may traverse before it is dropped. The default is 20.

Table 6-38 MSTP/RSTP Configuration Menu Options (/cfg/l2/mrst)

Command Syntax and Usage	
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 STG 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]	
<code>brg</code>	- CIST Bridge parameter menu
<code>port</code>	- CIST Port parameter menu
<code>add</code>	- Add VLAN(s) to CIST
<code>default</code>	- Default Common Internal Spanning Tree and Member parameters
<code>cur</code>	- Display current CIST parameters

[Table 6-39](#) 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 6-39 CIST Menu Options (`/cfg/l2/mrst/cist`)

Command Syntax and Usage	
brg	Displays the CIST Bridge Menu. To view menu options, see page 227 .
port <i><port alias or number></i>	Displays the CIST Port Menu. To view menu options, see page 228 .
add <i><VLAN numbers></i>	Adds selected VLANs to the CIST.
default	Resets all CIST parameters to their default values.
cur	Displays the current CIST configuration.

/cfg/l2/mrst/cist/brg

CIST Bridge Configuration

[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 6-40 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 alias or number> CIST Port Configuration

```
[CIST Port 1 Menu]
prior    - Set port Priority (0-240)
cost     - Set port Path Cost (1-2000000000, 0 for auto)
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 6-41 CIST Port Configuration Menu Options (/cfg/l2/mrst/cist/port)

Command Syntax and Usage

prior <0-240>

Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 240, in steps of 16 (0, 16, 32...), and the default is 128.

cost <0-2000000000>

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 2000 for 10 Gigabit ports, 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 6-41 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 <STP group number>

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). STP is used to prevent loops in the network topology. Up to 128 Spanning Tree Groups can be configured on the switch (STG 128 is reserved for management).

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

Table 6-42 Spanning Tree Configuration Menu (/cfg/l2/stg)

Command Syntax and Usage

brg

Displays the Bridge Spanning Tree Menu. To view menu options, see [page 232](#).

port <port alias or number>

Displays the Spanning Tree Port Menu. To view menu options, see [page 234](#).

add <VLAN number (1-4094)>

Associates a VLAN with a spanning tree and requires an external VLAN ID as a parameter.

remove <VLAN number (1-4094)>

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. STG is turned on by default.

off

Globally disables Spanning Tree Protocol.

Table 6-42 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 <STP group number> /brg Spanning Tree Bridge 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 6-43 Spanning Tree Bridge Menu Options (/cfg/l2/stg/brg)

Command Syntax and Usage

prior *<new bridge priority (0-65535)>*

Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STG root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The 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 226](#)).

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 226](#)).

Table 6-43 Spanning Tree Bridge Menu Options (/cfg/l2/stg/brg)

Command Syntax and Usage

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 226](#)).

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.

cur

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 number> /**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 (1-65535 (802.1d) /
              1-200000000 (MSTP/RSTP) /0 for auto)
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 6-44 Spanning Tree Port Menu Options (/cfg/l2/stg/port)

Command Syntax and Usage

prior <new port Priority (0-255)>

Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The default value is 128.

RSTP/MSTP: The range is 0 to 240, in steps of 16 (0, 16, 32...) 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 default is 19 for 100Mbps ports, 4 for 1Gb ports. A value of 0 (zero) 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 6-44 Spanning Tree Port Menu Options (/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/12/fdb
Forwarding Database Configuration

[FDB Menu]	
static	- Static FDB Menu
learn	- Enable/disable FDB Learning for all ports
flood	- Enable/disable Flooding of Unknown Destination MACs
cur	- Display current FDB configuration

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

Table 6-45 FDB Menu Options (/cfg/12/fdb)

Command Syntax and Usage	
static	Displays the static FDB menu. To view menu options, see page 237 .
learn disable enable	Enables or disables FDB learning. The default value is enabled.
flood disable enable	Enables or disables flooding of packets with unknown MAC addresses to all ports. The default value is enabled. Note: If you disable FDB flooding, you must also disable FDB learning.
cur	Display current FDB configuration.
NOTE – If you disable FDB learning and FDB flooding, manually add static MAC address entries for the management module, blade servers, and other connected devices. The static entries ensure that the GbESM retains connectivity to those devices. Use the following command to add static MAC address entries: /cfg/12/fdb/static/add	

/cfg/l2/fdb/static
Static FDB Configuration

[Static FDB Menu]

add	- Add a permanent FDB entry
del	- Delete a static FDB entry
clear	- Clear static FDB entries
cur	- Display current static FDB configuration

Use the following commands to configure static entries in the FDB.

Table 6-46 Static FDB Menu Options (/cfg/l2/fdb/static)

Command Syntax and Usage

add <MAC address> <VLAN number> <port number>
Adds a permanent FDB entry.

del <MAC address> <VLAN number>
Deletes a permanent FDB entry.

clear <MAC address> | **all** {**mac** | **vlan** | **port**}
Clears static FDB entries.

cur
Display current static FDB configuration.

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

[Trunk group 1 Menu]	
add	- Add port to trunk group
rem	- Remove port from trunk group
ena	- Enable trunk group
dis	- Disable trunk group
del	- Delete trunk group
cur	- Display current Trunk Group configuration

Trunk groups can provide super-bandwidth connections between 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 13 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 six ports/trunks can belong to the same trunk group.
- Configure all ports in a trunk group with the same link configuration (speed, duplex, flow control).
- Trunking from non-Alteon devices must comply with Cisco® EtherChannel® technology.

By default, each trunk group is empty and disabled.

Table 6-47 Trunk Configuration Menu Options (/cfg/l2/trunk)

Command Syntax and Usage

add *<port alias or number>*

Adds a physical port to the current trunk group.

rem *<port alias or number>*

Removes a physical port from the current trunk group.

ena

Enables the current trunk group.

dis

Disables the current trunk group.

del

Removes the current trunk group configuration.

cur

Displays current trunk group parameters.

/cfg/l2/thash

IP Trunk Hash Configuration

```
[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. The trunk hash settings affect both static trunks and LACP trunks.

Table 6-48 IP Trunk Hash Menu Options (/cfg/l2/thash)

Command Syntax and Usage

set

Displays the Trunk Hash Settings menu. To view menu options, see [page 239](#).

cur

Display current trunk hash configuration.

/cfg/l2/thash/set

IP Trunk Hash

```
[set 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 IP trunk hash parameters for the GbESM.

Table 6-49 IP Trunk Hash Menu Options (/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

LACP Configuration

[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 6-50 LACP Menu Options (/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: It is recommended that you use a timeout value of **long**, to reduce LACPDU processing. If your GbESM's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.

port <port alias or number>

Displays the LACP Port menu. To view menu options, see [page 242](#).

cur

Display current LACP configuration.

/cfg/l2/lacp/port <port alias or number> LACP Port Configuration

```
[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 6-51 LACP Port Menu Options (/cfg/l2/lacp/port)

Command Syntax and Usage

mode *off|active|passive*

Set the LACP mode for this port, as follows:

- **off**
Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is **off**.
- **active**
Turn LACP on and set this port to active. Active ports initiate LACPDUs.
- **passive**
Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.

prio <1-65535>

Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 32768.

adminkey <1-65535>

Set the admin key for this port. Only ports with the same *admin key* and *oper key* (operational state generated internally) can form a LACP trunk group.

cur

Displays the current LACP configuration for this port.

/cfg/l2/failovr
Layer 2 Failover Configuration

[Failover Menu]

trigger

- Trigger Menu

vlan

- Globally turn VLAN Monitor ON/OFF

on

- Globally turn Failover ON

off

- Globally turn Failover OFF

cur

- Display current Failover configuration

Use this menu to configure Layer 2 Failover. For more information about Layer 2 Failover, see “High Availability” in the Alteon OS *Application Guide*.

Table 6-52 Layer 2 Failover Menu Options (/cfg/l2/failovr)

Command Syntax and Usage

trigger <1-8>
Displays the Failover Trigger menu. To view menu options, see [page 244](#).

vlan on|off
Globally turns VLAN monitor on or off. When the VLAN Monitor is on, the switch automatically disables only internal ports that belong to the same VLAN as ports in the failover trigger. The default value is off.

on
Globally turns Layer 2 failover on.

off
Globally turns Layer 2 failover off.

cur
Displays current Layer 2 failover parameters.

/cfg/l2/failovr/trigger

Failover Trigger Configuration

[Trigger 1 Menu]	
amon	- Auto Monitor Menu
limit	- Limit of Trigger
ena	- Enable Trigger
dis	- Disable Trigger
cur	- Display current Trigger configuration

Table 6-53 Failover Trigger Menu Options (/cfg/l2/failovr/trigger)

Command Syntax and Usage

amon	Displays the Auto Monitor menu for the selected trigger. To view menu options, see page 245 .
limit <0-5>	Configures the minimum number of operational links allowed within each trigger before the trigger initiates a failover event. If you enter a value of zero (0), the switch triggers a failover event only when no links in the trigger are operational.
ena	Enables the selected trigger.
dis	Disables the selected trigger.
cur	Displays the current failover trigger settings.

/cfg/l2/failovr/trigger/amon
Auto Monitor Configuration

[Auto Monitor Menu]	
addtrnk	- Add trunk to Auto Monitor
remtrnk	- Remove trunk from Auto Monitor
addkey	- Add LACP port adminkey to Auto Monitor
remkey	- Remove LACP port adminkey from Auto Monitor
cur	- Display current Auto Monitor configuration

Table 6-54 Auto Monitor Menu Options (/cfg/l2/failovr/trigger/amon)

Command Syntax and Usage

addtrnk <Trunk Group number (1-13)>
Adds a trunk group to the Auto Monitor.

remtrnk <Trunk Group number (1-13)>
Removes a trunk group from the Auto Monitor.

addkey <1-65535>
Adds a LACP admin key to the Auto Monitor. LACP trunks formed with this admin key will be included in the Auto Monitor.

remkey <1-65535>
Removes a LACP admin key from the Auto Monitor.

cur
Displays the current Auto Monitor settings.

/cfg/12/vlan <VLAN number> **VLAN Configuration**

[VLAN 1 Menu]	
pvlan	- Protocol VLAN Menu
privlan	- Private-VLAN 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
bwidth	- Bandwidth Management
mgmt	- Enable/Disable this VLAN as additional management VLAN
ena	- Enable VLAN
dis	- Disable VLAN
del	- Delete VLAN
cur	- Display current VLAN configuration

The commands in this menu configure VLAN attributes, change the status of each VLAN, change the port membership of each VLAN, and delete VLANs. For more information on configuring VLANs, see [“Setup Part 3: VLANs” on page 38](#).

By default, the VLAN menu option is disabled except VLAN 1, which is enabled all the time. Internal server ports (INTx) and external ports (EXTx) are in VLAN 1 by default. Up to 1024 VLANs can be configured on the GbESM.

Table 6-55 VLAN Configuration Menu Options (/cfg/12/vlan)

Command Syntax and Usage

pvlan <1-8>

Displays the Protocol-based VLAN menu. To view menu options, see [page 248](#).

privlan

Displays the Private VLAN menu. To view menu options, see [page 250](#).

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 [1-128]>

Assigns a VLAN to a Spanning Tree Group.

add <port alias or number>

Adds port(s) to the VLAN membership.

Table 6-55 VLAN Configuration Menu Options (/cfg/l2/vlan)

Command Syntax and Usage

rem *<port alias or number>*

Removes port(s) from this VLAN.

def *<list of port numbers>*

Defines which ports are members of this VLAN. Every port must be a member of at least one VLAN. By default, internal server ports (INTx) and external ports (EXTx) are in VLAN 1.

bwidthDisplays the VLAN Bandwidth Management menu. To view menu options, see [page 251](#).**mgmt enable|disable**

Configures this VLAN as a management VLAN. You must add the management ports (MGT1 and MGT2) to each new management VLAN. External ports cannot be added to management VLANs.

ena

Enables this VLAN.

dis

Disables this VLAN without removing it from the configuration.

del

Deletes this VLAN.

cur

Displays the current VLAN configuration.

NOTE – All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. You cannot remove a port from VLAN 1 if the port has no membership in any other VLAN. Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on (see the `tag` command on [page 207](#)).

/cfg/l2/vlan/pvlan *<protocol number>*

Protocol-based VLAN Configuration

```
[VLAN 1 Protocol 1 Menu]
  pty      - Set protocol type
  prio     - Set priority to protocol
  add      - Add port to PVLAN
  rem      - Remove port from PVLAN
  ports    - Add/Remove a list of ports to/from PVLAN
  tagpvl   - Enable/Disable port tagging for PVLAN
  taglist  - Enable tagging a port list for PVLAN
  ena      - Enable protocol
  dis      - Disable protocol
  del      - Delete protocol
  cur      - Display current PVLAN configuration
```

Use this menu to configure Protocol-based VLAN (PVLAN) for the selected VLAN.

Table 6-56 PVLAN Menu Options (/cfg/l2/vlan/pvlan)

Command Syntax and Usage

pty *<(Ether2/SNAP/LLC)>* *<Ethernet type>*

Configures the frame type and the Ethernet type for the selected protocol. Ethernet type consists of a 4-digit (16 bit) hex code, such as 0080 (IPv4).

prio *<0-7>*

Configures the priority value for this PVLAN.

add

Adds a port to the selected PVLAN.

rem

Removes a port from the selected PVLAN.

ports

Defines a list of ports that belong to the selected protocol on this VLAN. Enter 0 (zero) to remove all ports.

tagpvl **enable|disable**

Enables or disables port tagging on this PVLAN.

taglist

Defines a list of ports that will be tagged by the selected protocol on this VLAN. Enter empty to disable tagging on all ports by this PVLAN.

ena

Enables the selected protocol on the VLAN.

Table 6-56 PVLAN Menu Options (/cfg/l2/vlan/pvlan)

Command Syntax and Usage	
dis	Disables the selected protocol on the VLAN.
del	Deletes the selected protocol configuration from the VLAN.
cur	Displays current parameters for the selected PVLAN.

/cfg/l2/vlan/privlan

Private VLAN Configuration

[privlan Menu]	
type	- Set Private-VLAN type
map	- Associate secondary VLAN with a primary VLAN
ena	- Enable Private-VLAN
dis	- Disable Private-VLAN
cur	- Display current Private-VLAN configuration

Use this menu to configure a Private VLAN.

Table 6-57 Private VLAN Menu Options (/cfg/l2/vlan/privlan)

Command Syntax and Usage

type **primary|isolated|community**

Defines the VLAN type, as follows:

- **Primary:** A Private VLAN must have only one primary VLAN. The primary VLAN carries unidirectional traffic to ports on the isolated VLAN or to community VLAN.
- **Isolated:** The isolated VLAN carries unidirectional traffic from host ports. A Private VLAN may have only one isolated VLAN.
- **Community:** Community VLANs carry upstream traffic from host ports. A Private VLAN may have multiple community VLANs.

map <2-4094>

Configures Private VLAN mapping between a secondary VLAN (*isolated* or *community*) and a primary VLAN. Enter the primary VLAN ID.

ena

Enables the Private VLAN.

dis

Disables the Private VLAN.

cur

Displays current parameters for the selected Private VLAN.

/cfg/l2/vlan/bwidth

VLAN Bandwidth Management Configuration

[Bandwidth Management Menu]	
ena	- Enable bandwidth management
dis	- Disable bandwidth management
rate	- Set bandwidth rate in KiloBits/s
mbsize	- Set maximum burst size in KiloBits
cur	- Display current bandwidth management parameters

Use this menu to configure Bandwidth Management on the VLAN. For each internal port in the VLAN that has Bandwidth Management enabled, an Access Control List (ACL) is used to set the bandwidth parameters.

Table 6-58 VLAN Bandwidth Management Menu Options (/cfg/l2/vlan/bwidth)

Command Syntax and Usage

ena

Enables Bandwidth Management on the VLAN.

dis

Disables Bandwidth Management on the VLAN.

rate <64-14000000>

Configures the traffic flow committed rate, in Kilobits per second.

To calculate the traffic flow rate, multiply 64 kbps by the total number of ports in the VLAN. Acceptable rate values will be a multiple of the result.

mbsize <32-57344>

Configures the maximum burst size, in Kilobits.

To calculate the maximum burst size, multiply one of the following discreet values by the total number of ports in the VLAN:
32, 64, 128, 256, 512, 1024, 2048, 4096

cur

Displays current Bandwidth Management parameters for the VLAN.

/cfg/l3

Layer 3 Configuration

```
[Layer 3 Menu]
  if          - Interface Menu
  gw          - Default Gateway Menu
  route       - Static Route Menu
  mroute      - Static IP Multicast Route Menu
  arp         - ARP Menu
  frwd        - Forwarding Menu
  nwf         - Network Filters Menu
  rmap        - Route Map Menu
  rip         - Routing Information Protocol Menu
  ospf        - Open Shortest Path First (OSPF) Menu
  bgp         - Border Gateway Protocol Menu
  igmp        - IGMP Menu
  dns         - Domain Name System Menu
  bootstrap  - Bootstrap Protocol Relay Menu
  vrrp        - Virtual Router Redundancy Protocol Menu
  rtrid       - Set router ID
  cur         - Display current IP configuration
```

Table 6-59 Layer 3 Configuration Menu (/cfg/l3)

Command Syntax and Usage

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

Displays the IP Interface Menu. To view menu options, see [page 254](#).

gw *<default gateway number (1-132)>*

Displays the IP Default Gateway Menu. To view menu options, see [page 255](#).

route

Displays the IP Static Route Menu. To view menu options, see [page 257](#).

mroute

Displays the Static IP Multicast Route Menu. To view menu options, see [page 258](#).

arp

Displays the Address Resolution Protocol Menu. To view menu options, see [page 259](#).

frwd

Displays the IP Forwarding Menu. To view menu options, see [page 261](#).

nwf *<Network filter number (1-256)>*

Displays the Network Filter Configuration Menu. To view menu options see [page 262](#).

Table 6-59 Layer 3 Configuration Menu (/cfg/l3)

Command Syntax and Usage

rmap *<route map number (1-32)>*Displays the Route Map Menu. To view menu options see [page 263](#).

ripDisplays the Routing Interface Protocol Menu. To view menu options, see [page 267](#).

ospfDisplays the OSPF Menu. To view menu options, see [page 270](#).

bgpDisplays the Border Gateway Protocol Menu. To view menu options, see [page 280](#).

igmpDisplays the IGMP Menu. To view menu options, see [page 286](#).

dnsDisplays the IP Domain Name System Menu. To view menu options, see [page 296](#).

bootpDisplays the Bootstrap Protocol Menu. To view menu options, see [page 297](#).

vrrpDisplays the Virtual Router Redundancy Configuration Menu. To view menu options, see [page 298](#).

rtrid *<IP address (such as, 192.4.17.101)>*Sets the router ID.

curDisplays 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 6-60 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 (1-4094)>*

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.

Table 6-60 IP Interface Menu Options (/cfg/l3/if)**Command Syntax and Usage****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 6-61 Default Gateway Menu Options (/cfg/l3/gw)**Command Syntax and Usage****addr** <default gateway address (such as, 192.4.17.44)>

Configures the IP address of the default IP gateway using dotted decimal notation.

intr <0-60 seconds>

The switch pings the default gateway to verify that it's up. The **intr** option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.

retry <number of attempts (1-120)>

Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.

arp disable|enable

Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default.

Table 6-61 Default Gateway Menu Options (/cfg/l3/gw)

Command Syntax and Usage	
vlan <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.

/cfg/l3/route
IP Static Route Configuration

[IP Static Route Menu]	
add	- Add static route
rem	- Remove static route
clear	- Clear static routes
interval	- Change ECMP route health check ping interval
retries	- Change the number of retries for ECMP health check
cur	- Display current static route configuration

Up to 128 static routes can be configured.

Table 6-62 IP Static Route Configuration Menu Options (cfg/l3/route)

Command Syntax and Usage

add <destination IP address> <mask> <gateway IP address> [*<interface number>*]

Adds a static route. You will be prompted to enter a destination IP address, destination subnet mask, and gateway IP address. Enter all addresses using dotted decimal notation.

Note: You may add multiple routes with the same IP address, but with different gateways. These routes become Equal Cost Multipath (ECMP) routes. The maximum number of gateways for each destination is five (5).

rem <destination IP address> <mask> [*<gateway IP address>*]

Removes a static route. Use dotted decimal notation to specify the destination address and subnet mask of the route.

Note: The gateway IP address is optional. Include the gateway when you remove an ECMP route. If you do not include the gateway, then all ECMP paths for the route are deleted.

clear <destination IP address> [*<gateway IP address>*] **all** <value>

Clears the selected IP static routes.

Note: Use the gateway IP address to clear a single gateway for an ECMP route.

interval <1-60>

Configures the ping interval for ECMP health checks, in seconds. The default value is one second.

retries <1-60>

Configures the number of health check retries allowed before the switch declares that the gateway is down. The default value is three (3).

cur

Displays the current IP static routes and any dynamically created BGP to ECMP routes.

In a BGP advertisement, if the advertised route's next hop matches the destination of the static configured route, the switch will create static ECMP routes with destinations equal to the advertised route and gateway of the matched static route's gateway.

/cfg/l3/mroute
IP Multicast Route Configuration

[IPMC Static Route Menu]	
add	- Add static IP Multicast route
rem	- Remove static IP Multicast route
cur	- Display current static IPMC route configuration

The following table describes the IP Multicast Route menu options.

Table 6-63 IP Static Route Configuration Menu Options (cfg/l3/mroute)

Command Syntax and Usage	
add <i><IPMC destination></i> <i><vlan></i> <i><port></i> primary backup host <i><virtual router id/none></i>	Adds a static multicast route. You will be prompted to enter a destination IP address (in dotted decimal notation), VLAN, and member port. Indicate whether the route is used for a primary, backup, or host multicast router.
rem <i><IPMC destination></i> <i><vlan></i> <i><port></i> primary backup host <i><virtual router id/none></i>	Removes a static multicast route. The destination address, VLAN, and member port of the route to remove must be specified.
cur	Displays the current IP multicast routes.

/cfg/l3/arp
ARP Configuration

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 6-64 ARP Configuration Menu Options (/cfg/l3/arp)

Command Syntax and Usage	
static	Displays Static ARP menu. To view options, see page 260 .
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

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
clear	- Clear static ARP entries
cur	- Display current static ARP configuration

Table 6-65 ARP Static Configuration Menu Options (/cfg/l3/arp/static)

Command Syntax and Usage

add *<IP address> <MAC address> <VLAN number> <port number>*
Adds a permanent ARP entry.

del *<IP address (such as, 192.4.17.101)>*
Deletes a permanent ARP entry.

clear [*<interface number>|<VLAN number>|<port number>|all*] *<ARP entry number>*
Clears static ARP entries.

cur
Displays current static ARP configuration.

/cfg/l3/frwd
IP Forwarding Configuration

[IP Forwarding Menu]	
dirbr	- Enable or disable forwarding directed broadcasts
noicmp	- Enable/disable No ICMP Redirects
on	- Globally turn IP Forwarding ON
off	- Globally turn IP Forwarding OFF
cur	- Display current IP Forwarding configuration

Table 6-66 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.	
noicmp	disable enable
Enables or disables ICMP re-directs. 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
  current   - Display current Network Filter configuration
```

Table 6-67 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.

current

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
current	- Display current route map configuration

Routing maps control and modify routing information.

Table 6-68 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 265](#).

aspath *<number 1-8>*

Displays the Autonomous System (AS) Filter menu. For more information, see [page 266](#).

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 *<(1-4294967294)>* | **none**

Sets the metric of the matched route.

type *<value (1/2)>* | **none**

Assigns the type of OSPF metric. The default is type 1.

- Type 1—External routes are calculated using both internal and external metrics.
 - Type 2—External routes are calculated using only the external metrics. Type 1 routes have more cost than Type 2.
 - none—Removes the OSPF metric.
-

Table 6-68 Routing Map Menu Options (/cfg/l3/rmap) (Continued)

Command Syntax and Usage	
prec <value (1-255)>	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.
current	Displays the current route configuration.

/cfg/l3/rmap *<route map number>* **/alist** *<access list number>*

IP Access List Configuration

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

current - Display current Access List configuration

Table 6-69 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 262 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.

current
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
current	- Display current AS Filter configuration

Table 6-70 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 (RIP) parameters. This option is turned off by default.

Table 6-71 RIP Menu Options (/cfg/l3/rip)

Command Syntax and Usage

if <1-127>	Displays the RIP Interface menu. For more information, see page 268 .
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
  poison     - Enable/disable poisoned reverse
  split      - Enable/disable split horizon
  triggl     - Enable/disable triggered updates
  mcast      - Enable/disable multicast updates
  default    - Set default route action
  metric     - Set metric
  auth       - Set authentication type
  key        - Set authentication key
  enable     - Enable interface
  disable    - Disable interface
  current    - Display current RIP interface configuration
```

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

NOTE – Do not configure RIP version 1 parameters if your routing equipment uses RIP version 2.

Table 6-72 RIP Interface Menu Options (/cfg/l3/rip/if)

Command Syntax and Usage

version 1|2|both

Configures the RIP version used by this interface. The default value is version 2.

supply disable|enable

When enabled, the switch supplies routes to other routers. The default setting is enabled.

listen disable|enable

When enabled, the switch learns routes from other routers. The default setting is enabled.

poison disable|enable

When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default setting is disabled.

split disable|enable

Enables or disables split horizon. The default setting is enabled.

Table 6-72 RIP Interface Menu Options (/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 setting is enabled.

mcast disable|enable

Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default setting is enabled.

default none|listen|supply|both

Configures the default route action. The default setting is none.

metric <1-15>

Configures the route metric, which indicates the relative distance to the destination. The default value is 1.

auth none|password

Configures the authentication type. The default is none.

key

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 6-73 OSPF Configuration Menu (/cfg/l3/ospf)

Command Syntax and Usage

aindex *<area index (0-2)>*

Displays the area index menu. This area index does not represent the actual OSPF area number. See [page 272](#) to view menu options.

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

Displays summary routes menu for up to 16 IP addresses. See [page 273](#) to view menu options.

if *<interface number (1-127)>*

Displays the OSPF interface configuration menu. See [page 274](#) to view menu options.

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

Displays the Virtual Links menu used to configure OSPF for a Virtual Link. See [page 276](#) to view menu options.

md5key *<key ID (1-255)>*

Assigns a string to MD5 authentication key.

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 277](#) to view menu options.

redist *fixed|static|rip|ebgp|ibgp*

Displays Route Distribution Menu. See [page 278](#) to view menu options.

lsdb *<LSDB limit (0-2000, 0 for no limit)>*

Sets the link state database limit.

Table 6-73 OSPF Configuration Menu (/cfg/l3/ospf)

Command Syntax and Usage	
default <metric (1-16777214)> <metric-type 1/2> none	Sets one default route among multiple choices in an area. Use none for no default.
on	Enables OSPF on the GbE Switch Module.
off	Disables OSPF on the GbE Switch Module.
cur	Displays the current OSPF configuration settings.

/cfg/l3/ospf/aindex <area index> Area Index Configuration

```
[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 6-74 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 (1-255)>

Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.

Table 6-74 Area Index Configuration Menu Options (/cfg/l3/ospf/aindex)

Command Syntax and Usage	
enable	Enables the OSPF area.
disable	Disables the OSPF area.
delete	Deletes the OSPF area.
cur	Displays the current OSPF configuration.

/cfg/l3/ospf/range *<range number>*
OSPF Summary Range Configuration

```
[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 6-75 OSPF Summary Range Configuration Menu Options (/cfg/l3/ospf/range)

Command Syntax and Usage	
addr <i><IP Address (such as, 192.4.17.101)></i>	Configures the base IP address for the range.
mask <i><IP address (such as, 192.4.17.101)></i>	Configures the IP address mask for the range.
aindex <i><area index (0-2)></i>	Configures the area index used by the GbE Switch Module.
hide disable enable	Hides the OSPF summary range.
enable	Enables the OSPF summary range.

Table 6-75 OSPF Summary Range Configuration Menu Options (/cfg/l3/ospf/range)**Command Syntax and Usage****disable**

Disables the OSPF summary range.

delete

Deletes the OSPF summary range.

current

Displays the current OSPF summary range.

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

OSPF Interface Configuration

```
[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 6-76 OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)**Command Syntax and Usage****aindex** *<area index (0-2)>*

Configures the OSPF area index.

prio *<priority value (0-255)>*

Configures the priority value for the GbE Switch Module's OSPF interfaces.

(A priority value of 255 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)

cost *<cost value (1-65535)>*

Configures cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.

Table 6-76 OSPF Interface Configuration Menu Options (/cfg/l3/ospf/if)

Command Syntax and Usage

hello <value (1-65535)>Configures the interval in seconds between the `hello` packets for the interfaces.**dead** <value (1-65535)>Configures 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 (1-3600)>

Configures the transit delay in seconds.

retra <value (0-3600)>

Configures the retransmit interval in seconds.

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.

curDisplays the current settings for OSPF interface.

/cfg/l3/ospf/virt *<link number>*

OSPF Virtual Link Configuration

```
[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 6-77 OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt)

Command Syntax and Usage

aindex *<area index (0-2)>*

Configures the OSPF area index.

hello *<value (1-65535)>*

Configures the authentication parameters of a hello packet, in seconds.

dead *<value (1-65535)>*

Configures the health parameters of a hello packet, in seconds. Default is 60 seconds.

trans *<value (1-3600)>*

Configures the delay in transit, in seconds. Default is one second.

retra *<value (1-3600)>*

Configures the retransmit interval, in seconds. Default is five seconds.

nbr *<NBR router ID (IP address)>*

Configures the router ID of the virtual neighbor. Default is 0.0.0.0.

key *<password>*

Configures the password (up to eight characters) for each virtual link. Default is none.

mdkey *<key ID (1-255)>* | **none**

Sets MD5 key ID for each virtual link. Default is none.

enable

Enables OSPF virtual link.

Table 6-77 OSPF Virtual Link Configuration Menu Options (/cfg/l3/ospf/virt)**Command Syntax and Usage****disable**

Disables OSPF virtual link.

delete

Deletes OSPF virtual link.

cur

Displays the current OSPF virtual link settings.

/cfg/l3/ospf/host *<host number>*

OSPF Host Entry Configuration

```
[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 6-78 OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)**Command Syntax and Usage****addr** *<IP address (such as, 192.4.17.101)>*

Configures the base IP address for the host entry.

aindex *<area index (0-2)>*

Configures the area index of the host.

cost *<cost value (1-65535)>*

Configures the cost value of the host.

enable

Enables OSPF host entry.

disable

Disables OSPF host entry.

Table 6-78 OSPF Host Entry Configuration Menu Options (/cfg/l3/ospf/host)

Command Syntax and Usage	
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

[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 6-79 OSPF Route Redistribution Menu Options (/cfg/l3/ospf/redist)

Command Syntax and Usage	
add (<route map (1-32)> <route map (1-32)>)... all	Adds selected routing maps to the rmap list. To add all the 32 route maps, enter all . To add specific route maps, enter routing map numbers one per line, NULL at the end. This option adds a route map to the route redistribution list. The routes of the redistribution protocol matched by the route maps in the route redistribution list will be redistributed.
rem (<route map (1-32)> <route map (1-32)>) ... all	Removes the route map from the route redistribution list. Removes routing maps from the rmap list. To remove all 32 route maps, enter all . To remove specific route maps, enter routing map numbers one per line, NULL at end.
export <metric (1-16777214)><metric type [1/2]> none	Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter none .
cur	Displays the current route map settings.

/cfg/13/ospf/md5key *<key ID>*
OSPF MD5 Key Configuration

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

Table 6-80 OSPF MD5 Key Configuration Menu Options (/cfg/ip/ospf/md5key)

Command Syntax and Usage

- | | |
|---------------|--|
| key | Sets the authentication key for this OSPF packet. |
| <hr/> | |
| delete | Deletes the authentication key for this OSPF packet. |
| <hr/> | |
| cur | Displays the current MD5 key configuration. |
| <hr/> | |

/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.

BGP commands enable you to configure the switch to receive routes and to advertise static routes, fixed routes and virtual server IP addresses with other internal and external routers. In the current Alteon OS implementation, the GbE Switch Module does not advertise BGP routes that are learned from one iBGP *speaker* to another iBGP *speaker*.

BGP is turned off by default.

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

Table 6-81 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 282](#).

aggr <aggregate number (1-16)>

Displays the Aggregation Menu. To view menu options, see [page 285](#).

Table 6-81 Border Gateway Protocol Menu (/cfg/l3/bgp)

Command Syntax and Usage	
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

```
[BGP Peer 1 Menu]
  redistribute - 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 6-82 BGP Peer Configuration Menu Options (/cfg/l3/bgp/peer)

Command Syntax and Usage

redist

Displays BGP Redistribution Menu. To view the menu options, see [page 284](#).

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 (1-65535)>

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. The default value is 180 seconds.

alive <keep alive time (0-21845)>

Sets the keep-alive time for the specified peer, in seconds. The default value is 60 seconds.

Table 6-82 BGP Peer Configuration Menu 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.

Note: The TTL value is significant only to eBGP peers, for iBGP peers the TTL value in the IP packets is always 255 (regardless of the configured value).

addi *<route map ID (1-32)>*

Adds route map into in-route map list.

addo *<route map ID (1-32)>*

Adds route map into out-route map list.

remi *<route map ID (1-32)>*

Removes route map from in-route map list.

remo *<route map ID (1-32)>*

Removes route map from out-route map list.

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

```
[Redistribution Menu]
metric - Set default-metric of advertised routes
default - Set default route action
rip - Enable/disable advertising RIP routes
ospf - Enable/disable advertising OSPF routes
fixed - Enable/disable advertising fixed routes
static - Enable/disable advertising static routes
cur - Display current redistribution configuration
```

Table 6-83 BGP Redistribution Menu Options (/cfg/l3/bgp/peer/redist)

Command Syntax and Usage

metric <metric (1-4294967294)> | **none**

Sets default metric of advertised routes.

default **none** | **import** | **originate** | **redistribute**

Sets default route action.

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 if it does not have any default routes in its routing table.

Redistribute: Default routes are either configured through default gateway or learned through other protocols and redistributed to peer. If the routes are learned from default gateway configuration, you have to enable static routes since the routes from default gateway are static routes. Similarly, if the routes are learned from a certain routing protocol, you have to enable that protocol in this redistribute submenu.

rip **disable** | **enable**

Enables or disables advertising RIP routes

ospf **disable** | **enable**

Enables or disables advertising OSPF routes.

fixed **disable** | **enable**

Enables or disables advertising fixed routes.

static **disable** | **enable**

Enables or disables advertising static routes.

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 BGP aggregation to specify the routes/range of IP destinations a peer router accepts from other peers. All matched routes are aggregated to one route, to reduce the size of the routing table. By default, the first aggregation number is enabled and the rest are disabled.

Table 6-84 BGP Aggregation Configuration Menu Options (/cfg/l3/bgp/aggr)

Command Syntax and Usage

addr	<i><IP address (such as 192.4.17.101)></i> Defines the starting subnet IP address for this aggregation, using dotted decimal notation. The default address is 0.0.0.0.
mask	<i><IP subnet mask (such as, 255.255.255.0)></i> This IP address mask is used with addr to define the range of IP addresses that will be aggregated to one route when the aggregation is enabled. The default address is 0.0.0.0.
ena	Enables this BGP aggregation.
dis	Disables this BGP aggregation.
del	Deletes this BGP aggregation.
cur	Displays the current BGP aggregation configuration.

/cfg/l3/igmp

IGMP Configuration

[IGMP Menu]	
snoop	- IGMP Snoop Menu
relay	- IGMP Relay Menu
mrouter	- Static Multicast Router Menu
igmpflt	- IGMP Filtering Menu
adv	- IGMP Advanced Menu
on	- Globally turn IGMP ON
off	- Globally turn IGMP OFF
cur	- Display current IGMP configuration

Table 6-85 describes the commands used to configure basic IGMP parameters.

Table 6-85 IGMP Menu Options (/cfg/l3/igmp)

Command Syntax and Usage

snoop

Displays the IGMP Snoop Menu. To view menu options, see [page 287](#).

relay

Displays the IGMP Relay Menu. To view menu options, see [page 289](#).

mrouter

Displays the Static Multicast Router Menu. To view menu options, see [page 291](#).

igmpflt

Displays the IGMP Filtering Menu. To view menu options, see [page 292](#).

adv

Displays the IGMP Advanced Menu. To view menu options, see [page 295](#).

on

Globally turns IGMP on.

off

Globally turns IGMP off.

cur

Displays the current IGMP configuration parameters.

/cfg/l3/igmp/snoop
IGMP Snooping Configuration

[IGMP Snoop Menu]	
igmpv3	- IGMP Version3 Snoop Menu
mrto	- Set multicast router timeout
aggr	- Aggregate IGMP report
srcip	- Set source ip to use when proxying GSQ
add	- Add VLAN(s) to IGMP Snooping
rem	- Remove VLAN(s) from IGMP Snooping
clear	- Remove all VLAN(s) from IGMP Snooping
ena	- Enable IGMP Snooping
dis	- Disable IGMP Snooping
cur	- Display current IGMP Snooping configuration

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

Table 6-86 describes the commands used to configure IGMP Snooping.

Table 6-86 IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage	
igmpv3	Displays the IGMP version 3 Menu. To view menu options, see page 288 .
mrto <1-600 seconds>	Configures the timeout value for IGMP Membership Queries (mrrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 600 seconds. The default is 255 seconds.
aggr enable disable	Enables or disables IGMP Membership Report aggregation.
srcip <IP address (such as, 192.4.17.101)>	Configures the source IP address used as a proxy for IGMP Group Specific Queries.
add <VLAN number (1-4094)>	Adds the selected VLAN(s) to IGMP Snooping.
rem <VLAN number (1-4094)>	Removes the selected VLAN(s) from IGMP Snooping.
clear	Removes all VLANs from IGMP Snooping.

Table 6-86 IGMP Snoop Menu Options (/cfg/l3/igmp/snoop)

Command Syntax and Usage	
ena	Enables IGMP Snooping.
dis	Disables IGMP Snooping.
cur	Displays the current IGMP Snooping parameters.

/cfg/l3/igmp/snoop/igmpv3
IGMP Version 3 Configuration

[IGMP V3 Snoop Menu]	
sources	- Set the number of sources to snoop in group record
v1v2	- Enable/disable snooping IGMPv1/v2 reports
exclude	- Enable/disable snooping EXCLUDE mode reports
ena	- Enable IGMPv3 Snooping
dis	- Disable IGMPv3 Snooping
cur	- Display current IGMP Snooping V3 configuration

Table 6-89 describes the commands used to configure IGMP version 3.

Table 6-87 IGMP V3 Menu Options (/cfg/l3/igmp/snoop/igmpv3)

Command Syntax and Usage	
sources <1-64>	Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control.
v1v2 enable disable	Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is enabled.
exclude enable disable	Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.
ena	Enables IGMP version 3. The default value is disabled .

Table 6-87 IGMP V3 Menu Options (/cfg/l3/igmp/snoop/igmpv3)

Command Syntax and Usage

dis

Disables IGMP version 3.

cur

Displays the current IGMP version 3 configuration.

/cfg/l3/igmp/relay

IGMP Relay Configuration

[IGMP Relay Menu]

mrtr	- Upstream Multicast Router Menu
add	- Add VLAN(s) to downstream
rem	- Remove VLAN(s) from downstream
clear	- Remove all VLAN(s) from downstream
report	- Set unsolicited report interval
ena	- Enable IGMP Relay
dis	- Disable IGMP Relay
cur	- Display current IGMP Relay configuration

[Table 6-89](#) describes the commands used to configure IGMP Relay.

Table 6-88 IGMP Relay Menu Options (/cfg/l3/igmp/relay)

Command Syntax and Usage

mrtr <multicast router number (1-2)>

Displays the Upstream Multicast Router Menu. To view menu options, see [page 290](#).

add <VLAN number (1-4094)>

Adds the VLAN to the list of IGMP Relay VLANs.

rem <VLAN number (1-4094)>

Removes the VLAN from the list of IGMP Relay VLANs.

clear

Removes all VLANs from the list of IGMP Relay VLANs.

report <0-150>

Configures the interval between unsolicited Join reports sent by the switch, in seconds.
The default value is 10.

ena

Enables IGMP Relay.

Table 6-88 IGMP Relay Menu Options (/cfg/l3/igmp/relay)

Command Syntax and Usage	
dis	Disables IGMP Relay.
cur	Displays the current IGMP Relay configuration.

/cfg/l3/igmp/relay/mrtr <Mrouter number>
IGMP Relay Multicast Router Configuration

[Multicast router 2 Menu]	
addr	- Set IP address of multicast router
intr	- Set interval between ping attempts
retry	- Set number of failed attempts to declare router DOWN
restr	- Set number of successful attempts to declare router UP
version	- Set IGMP version
ena	- Enable multicast router
dis	- Disable multicast router
del	- Delete multicast router
cur	- Display current multicast router configuration

Table 6-91 describes the commands used to configure the IGMP Relay multicast router.

Table 6-89 IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr)

Command Syntax and Usage	
addr <IP address (such as 192.4.17.101)>	Configures the IP address of the IGMP multicast router used for IGMP Relay.
intr <1-60>	Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.
retry <1-120>	Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4.
restr <1-128>	Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5.
version <1-2>	Configures the IGMP version (1 or 2) of the multicast router.

Table 6-89 IGMP Relay Mrouter Menu Options (/cfg/l3/igmp/relay/mrtr)

Command Syntax and Usage	
ena	Enables the multicast router.
dis	Disables the multicast router.
del	Deletes the multicast router from IGMP Relay.
cur	Displays the current IGMP Relay multicast router parameters.

/cfg/l3/igmp/mrouter
IGMP Static Multicast Router Configuration

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

Table 6-90 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 6-90 IGMP Static Multicast Router Menu Options (/cfg/l3/igmp/mrouter)

Command Syntax and Usage	
add <port number> <VLAN number> <IGMP version number>	Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version (1, 2, or 3) of the multicast router.
remove <port number> <VLAN number> <IGMP version number>	Removes a static multicast router from the selected port/VLAN combination.
clear	Clears all static multicast routers from the switch.
cur	Displays the current IGMP Static Multicast Router parameters.

`/cfg/l3/igmp/igmpflt` IGMP Filtering Configuration

[IGMP Filter Menu]	
<code>filter</code>	- IGMP Filter Definition Menu
<code>port</code>	- IGMP Filtering Port Menu
<code>ena</code>	- Enable IGMP Filtering
<code>dis</code>	- Disable IGMP Filtering
<code>cur</code>	- Display current IGMP Filtering configuration

[Table 6-91](#) describes the commands used to configure an IGMP filter.

Table 6-91 IGMP Filtering Menu Options (`/cfg/l3/igmp/igmpflt`)

Command Syntax and Usage

filter *<filter number (1-16)>*

Displays the IGMP Filter Definition Menu. To view menu options, see [page 293](#).

port *<port number>*

Displays the IGMP Filtering Port Menu. To view menu options, see [page 294](#).

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 6-92 describes the commands used to define an IGMP filter.

Table 6-92 IGMP Filter Definition Menu Options (/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 alias or 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 6-93 describes the commands used to configure a port for IGMP filtering.

Table 6-93 IGMP Filter Port Menu Options (/cfg/l3/igmp/igmpflt/port)

Command Syntax and Usage

filt enable|disable

Enables or disables IGMP filtering on this port.

add *<filter number (1-16)>*

Adds an IGMP filter to this port.

rem *<filter number (1-16)>*

Removes an IGMP filter from this port.

cur

Displays the current IGMP filter parameters for this port.

/cfg/l3/igmp/adv
IGMP Advanced Configuration

[IGMP Advanced Menu]

qintrval

- Set IGMP query interval

robust

- Set expected packet loss on subnet

timeout

- Set report timeout

fastlv

- Enable/disable Fastleave processing in VLAN

flood

- Flood unregistered IPMC

cur

- Display current IGMP Advanced configuration

Table 6-91 describes the commands used to configure advanced IGMP parameters.

Table 6-94 IGMP Advanced Menu Options (/cfg/l3/igmp/adv)

Command Syntax and Usage

qinterval <1-600>

Configures the interval for IGMP Query Reports. The default value is 125 seconds.

robust <2-10>

Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The default value is 2.

timeout <1-255 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.

fastlv <VLAN number (1-4094)> **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.

flood **enable** | **disable**

Configures the switch to flood unregistered IP multicast reports to all ports. The default setting is **enabled**.

Note: If IGMP hosts reside on different VLANs, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs.

cur

Displays the current IGMP Advanced parameters.

/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 6-95 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 is turned off by default.

Table 6-96 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
  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 *Application Guide*.

Table 6-97 VRRP Menu Options (/cfg/l3/vrrp)

Command Syntax and Usage

vr <virtual router number (1-1024)>

Displays the VRRP Virtual Router Menu. This menu is used for configuring virtual routers on this switch. To view menu options, see [page 300](#).

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 303](#).

if <interface number (1-127)>

Displays the VRRP Virtual Router Interface Menu. To view menu options, see [page 306](#).

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 307](#).

Table 6-97 VRRP Menu Options (/cfg/l3/vrrp)

Command Syntax and Usage	
hotstan disable enable	Enables or disables hot standby processing, in which two or more switches provide redundancy for each other. By default, this option is disabled.
on	Globally enables VRRP on this switch.
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 reenter priority
  adver     - Set advertisement interval
  preem     - Enable or disable preemption
  ena       - Enable virtual router
  dis       - Disable virtual router
  del       - Delete virtual router
  cur       - Display current VRRP virtual router configuration
```

This menu is used for configuring virtual routers for this switch. A virtual router is defined by its virtual router ID and an IP address. On each VRRP-capable routing device participating in redundancy for this virtual router, a virtual router will be configured to share the same virtual router ID and IP address.

Virtual routers are disabled by default.

Table 6-98 VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr)

Command Syntax and Usage

track

Displays the VRRP Priority Tracking Menu for this virtual router. Tracking is 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 302](#).

vrid *<virtual router ID (1-1024)>*

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 virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 1024. The default value is 1.

All `vrid` values must be unique within the VLAN to which the virtual router's IP interface belongs.

addr *<IP address (such as, 192.4.17.101)>*

Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0.

Table 6-98 VRRP Virtual Router Menu Options (/cfg/l3/vrrp/vr)

Command Syntax and Usage

if *<interface number (1-127)>*

Selects a switch IP interface. If the IP interface has the same IP address as the **addr** option above, this switch is considered the “owner” of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must preempt another virtual router which has assumed master routing authority. This preemption occurs even if the **preem** option below is disabled. The default 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.

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 307](#)).

Criteria are tracked dynamically, continuously updating virtual router priority levels when enabled. If the virtual router preemption option (see *preem* in [Table 6-98 on page 300](#)) 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 6-99 Virtual Router Priority Tracking Menu 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 6-100 Virtual Router Group Menu Options (/cfg/l3/vrrp/group)

Command Syntax and Usage

track

Displays the VRRP Priority Tracking Menu for the virtual router group. Tracking is 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 305](#).

vrid <virtual router ID (1-1024)>

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 1024. 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 (1-127)>

Selects a switch IP interface. The default switch IP interface number is 1.

Table 6-100 Virtual Router Group Menu 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]	
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 6-101 Virtual Router Group Priority Tracking Menu (/cfg/l3/vr/group/track)

Command Syntax and Usage

ifs disable|enable

When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.

ports disable|enable

When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered “active” if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

cur

Displays the current configuration for priority tracking for this virtual router.

/cfg/l3/vrrp/if *<interface number>*
VRRP Interface Configuration

NOTE – The *interface-number* (1 to 127) 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 6-102 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 302](#)), the priority level for the virtual router is increased by an amount defined through this menu.

Table 6-103 VRRP Tracking Menu Options (/cfg/l3/vrrp/track)

Command Syntax and Usage

vrs <0-254>	Defines the priority increment value (0 through 254) for virtual routers in master mode detected on this switch. The default value is 2.
ifs <0-254>	Defines the priority increment value (0 through 254) for active IP interfaces detected on this switch. The default value is 2.
ports <0-254>	Defines the priority increment value (0 through 254) for active ports on the virtual router’s VLAN. The default value is 2.
cur	Displays the current configuration of priority tracking increment values.

NOTE – These priority tracking options only define increment values. These options do not affect the VRRP master router election process until options under the VRRP Virtual Router Priority Tracking Menu (see [page 302](#)) are enabled.

/cfg/qos

Quality of Service Configuration

[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 (DSCP) value of incoming packets. This allows you to differentiate between various types of traffic, and provide different priority levels.

Table 6-104 Quality of Service Menu Options (/cfg/qos)

Command Syntax and Usage

8021p

Displays 802.1p configuration menu. To view menu options, see [page 309](#).

dscp

Displays DSCP configuration menu. To view menu options, see [page 310](#).

/cfg/qos/8021p
802.1p Configuration

[802.1p Menu]

 priq - Set priority to COS queue mapping

 qweight - Set weight to a COS queue

 numcos - Set number of COS queue

 cur - Display current 802.1p configuration

This feature provides the capability to filter IP packets based on the 802.1p bits in the packet's VLAN header. The 802.1p bits specify the priority that you should give to the packets while forwarding them. The packets with a higher (non-zero) priority bits are given forwarding preference over packets with numerically lower priority bits value.

Table 6-105 802.1p Menu Options (/cfg/qos/8021p)

Command Syntax and Usage

priq <0-7> <0-1> <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 that handles the matching traffic.
qweight <0-1> <0-7> <0-15>
Configures the weight of the selected Class of Service queue (COSq). Enter the queue number, followed by the scheduling weight (0-15).
numcos 2 8
Sets the number of Class of Service queues for switch ports. The default value is 2. You must apply, save, and reset the switch to activate the new configuration.
cur
Displays the current 802.1p parameters.

/cfg/qos/dscp
DSCP Configuration

[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 6-106 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 (0-7)>	Maps the DiffServ Code point value to an 802.1p priority value. Enter the DSCP value, followed by the corresponding 802.1p value.
on	Turns on DSCP re-marking globally.
off	Turns off DSCP re-marking globally.
cur	Displays the current DSCP parameters.

/cfg/acl

Access Control List Configuration

[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 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 6-107 ACL Menu Options (/cfg/acl)

Command Syntax and Usage

acl <1-4096>
Displays Access Control List configuration menu. To view menu options, see page 312 .
block <1-4096>
Displays ACL Block configuration menu. To view menu options, see page 317 .
group <1-4096>
Displays ACL Group configuration menu. To view menu options, see page 318 .
cur
Displays the current ACL parameters.

/cfg/acl/acl <ACL number>

ACL Configuration

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

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

Table 6-108 ACL Menu Options (/cfg/acl/acl x)

Command Syntax and Usage

ethernet

Displays the ACL Ethernet Header menu. To view menu options, see [page 313](#).

ipv4

Displays the ACL IP Header menu. To view menu options, see [page 314](#).

tcpudp

Displays the ACL TCP/UDP Header menu. To view menu options, see [page 315](#).

pktfmt <packet format>

Displays the ACL Packet Format menu. To view menu options, see [page 316](#).

egrport <port alias or number>

Configures the ACL to function on egress packets.

action **permit** | **deny** | **setprio** <0-7>

Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the 802.1p priority level (0-7).

stats **enable** | **disable**

Enables or disables the statistics collection for the Access Control List.

reset

Resets the ACL parameters to their default values.

cur

Displays the current ACL parameters.

/cfg/acl/acl <ACL number>/ethernet
Ethernet Filtering Configuration

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 6-109 Ethernet Filtering Menu Options (/cfg/acl/acl x/ethernet)

Command Syntax and Usage

smac <MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>
Defines the source MAC address for this ACL.

dmac <MAC address (such as 00:60:cf:40:56:00)> <mask (FF:FF:FF:FF:FF:FF)>
Defines the destination MAC address for this ACL.

vlan <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 Configuration

[Filtering IPv4 Menu]	
sip	- Set to filter on source IP address
dip	- Set to filter on destination IP address
proto	- Set to filter on 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 6-110 IP version 4 Filtering Menu Options (/cfg/acl/acl x/ipv4)

Command Syntax and Usage

sip <IP address> <mask (such as 255.255.255.0)>

Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.

dip <IP address> <mask (such as 255.255.255.0)>

Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.

proto <0-255>

Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols.

<u>Number</u>	<u>Name</u>
---------------	-------------

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 Configuration

[Filtering TCP/UDP Menu]	
sport	- Set to filter on TCP/UDP source port
dport	- Set to filter on TCP/UDP destination port
flags	- Set to filter TCP/UDP flags
reset	- Reset all fields
cur	- Display current parameters

This menu allows you to define TCP/UDP matching criteria for an ACL.

Table 6-111 TCP/UDP Filtering Menu Options (/cfg/acl/acl x/tcpudp)

Command Syntax and Usage

sport <source port (1-65535)> <mask (0xFFFF)>

Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports:

<u>Number</u>	<u>Name</u>
20	ftp-data
21	ftp
22	ssh
23	telnet
25	smtp
37	time
42	name
43	whois
53	domain
69	tftp
70	gopher
79	finger
80	http

dport <destination port (1-65535)> <mask (0xFFFF)>

Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with **sport** above.

flags <value (0x0-0x3f)>

Defines a TCP/UDP flag for the ACL.

Table 6-111 TCP/UDP Filtering Menu 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 Configuration

[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 6-112 ACL Packet Format Filtering Menu 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 6-113 ACL Block Menu 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 Configuration

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

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

Table 6-114 ACL Group Menu Options (/cfg/acl/group x)

Command Syntax and Usage

add acl *<1-4096>*
Adds the selected ACL to the ACL Group.

rem acl *<1-4096>*
Removes the selected ACL from the ACL Group.

cur
Displays the current ACL group parameters.

/cfg/pmirr
Port Mirroring Configuration

```
[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 6-115 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 320](#).

cur
Displays current settings of the mirrored and monitoring ports.

/cfg/pmirr/monport

Port-Mirroring Configuration

[Port EXT1 Menu]	
add	- Add "Mirrored" port
rem	- Rem "Mirrored" port
delete	- Delete this "Monitor" port
cur	- Display current Port-based Port Mirroring configuration

Table 6-116 Port Mirroring Monitor Port Menu Options (/cfg/pmirr/monport)

Command Syntax and Usage

add *<mirrored port (port to mirror from)> <direction (in, out, or both)>*

Adds the port to be mirrored. This command also allows you to enter the direction of the traffic. It is necessary to specify the direction because:

If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the 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 322](#).

/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
prm	- Protected Mode Menu
passwd	- Change current user password
clrlog	- Clear syslog messages
conlog	- Enable/Disable Session Console Logging
cfgtrk	- Track last config change made
ntpreq	- Send NTP request

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

Table 7-1 Operations Menu (/oper)

Command Syntax and Usage

port *<port alias or number>*

Displays the Operational Port Menu. To view menu options, see [page 326](#).

vrrp

Displays the Operational Virtual Router Redundancy Menu. To view menu options, see [page 328](#).

ip

Displays the IP Operations Menu, which has one sub-menu/option, the Operational Border Gateway Protocol Menu. To view menu options, see [page 329](#).

ip

Displays the Protected Mode menu. To view menu options, see [page 330](#).

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.

conlog enable|disable

Enables or disables console logging of the current session.

cfgtrk

Displays a list of configuration changes made since the last `apply` command. Each time the `apply` command is sent, the configuration-tracking log is cleared.

Table 7-1 Operations Menu (/oper)

Command Syntax and Usage	
ntpreq	Allows the user to send requests to the NTP server.
prm	Displays the Protected Mode Menu. To view menu options, see page 330 .

/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 re-setting the 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 327 .
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 802.1x Menu Options (/oper/port x/8021x)

Command Syntax and Usage

reset

Re-initializes the 802.1X access-control parameters for the port. The following actions take place, depending on the 802.1X port configuration:

- **force unauth** - the port is placed in unauthorized state, and traffic is blocked.
- **auto** - the port is placed in unauthorized state, then authentication is initiated.
- **force auth** - the port is placed in authorized state, and authentication is not required.

reauth

Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1X mode is configured as auto.

/oper/vrrp

Operations-Level VRRP Options.

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

Table 7-4 Operations-Level VRRP Menu Options (/oper/vrrp)

Command Syntax and Usage	
back <virtual router number (1-1024)>	<p>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:</p> <ul style="list-style-type: none">■ 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 Operations-Level IP Menu Options (/oper/ip)

Command Syntax and Usage

bgp
Displays the Border Gateway Protocol Operations Menu. To view the menu options see [page 329](#).

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

Command Syntax and Usage

start *<peer number (1-16)>*
Starts the peer session.

stop *<peer number (1-16)>*
Stops the peer session.

cur
Displays the current BGP operational state.

/oper/prm

Protected Mode Options

```
[Protected Mode Menu]
mgt  - Enable/disable local control of external management
ext  - Enable/disable local control of external ports
fact - Enable/disable local control of factory default reset
mif  - Enable/disable local control of Mgmt VLAN interface
on   - Turn on/alter protected mode by applying enabled features
off  - Turn off protected mode by removing all features
cur  - Display current PRM configuration
```

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

Table 7-7 Protected Mode Options (/oper/prm)

Command Syntax and Usage

mgt enable|disable

Enables exclusive local control of switch management. When Protected Mode is set to **on**, the management module cannot be used to disable external management on the switch. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

ext enable|disable

Enables exclusive local control of external ports. When Protected Mode is set to **on**, the management module cannot be used to disable external ports on the switch. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

fact enable|disable

Enables exclusive local control of factory default resets. When Protected Mode is set to **on**, the management module cannot be used to reset the switch software to factory default values. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

mif enable|disable

Enables exclusive local control of the management interface (IF 128). When Protected Mode is set to **on**, the management module cannot be used to configure parameters for the management interface. The default value is **enabled**.

Note: Due to current management module implementation, this setting cannot be disabled.

on

Turns Protected Mode **on**. When Protected Mode is turned on, the switch takes exclusive local control of all enabled options.

Table 7-7 Protected Mode Options (/oper/prm)

Command Syntax and Usage	
off	Turns Protected Mode off . When Protected Mode is turned off, the switch relinquishes exclusive local control of all enabled options.
cur	Displays the current Protected Mode configuration.

CHAPTER 8

The Boot Options Menu

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

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

In addition to the Boot Menu, you can use a Web browser or SNMP to work with switch image and configuration files. To use SNMP, refer to [“Working with Switch Images and Configuration Files” on page 372](#).

/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
  mode  - Select CLI mode to use on next boot
  prompt - Prompt for selectable boot mode
  gting - 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-304.ibm.com/jct01004c/systems/support>

Click on **software updates**. Use the `/boot/cur` command to determine the current software version.

The typical upgrade process for the software image consists of the following steps:

- Place the new image onto a FTP or TFTP server on your network, or on a local computer.
- Transfer the new image to your switch.
- Select the new software image to be loaded into switch memory the next time the switch is reset.

Loading New Software to Your Switch

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

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

Using the BBI

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

- FTP server
- TFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. **Click the Configure context button in the toolbar.**
2. **In the Navigation Window, select System > Config/Image Control.**

The Switch Image and Configuration Management page appears.

Switch Image and Configuration Management									
Image 1 Version	version 1.5.0, downloaded 16:51:09 Sun Jan 8, 2008								
Image 2 Version	version 1.4.1, downloaded 14:08:11 Fri Jan 6, 2008								
Boot Version	version 1.5.0								
Active Image Version	1.5.0								
Next Boot Image Selection	image 1 ▼								
<table border="1"> <tr> <td>Active Configuration Block</td> <td>active config</td> </tr> <tr> <td>Next Boot Configuration Block Selection</td> <td>active config ▼</td> </tr> <tr> <td>Next CLI Boot Mode Selection</td> <td>AOS CLI ▼</td> </tr> <tr> <td>Prompt for selectable boot mode</td> <td>DISABLE ▼</td> </tr> </table>		Active Configuration Block	active config	Next Boot Configuration Block Selection	active config ▼	Next CLI Boot Mode Selection	AOS CLI ▼	Prompt for selectable boot mode	DISABLE ▼
Active Configuration Block	active config								
Next Boot Configuration Block Selection	active config ▼								
Next CLI Boot Mode Selection	AOS CLI ▼								
Prompt for selectable boot mode	DISABLE ▼								
<table border="1"> <tr> <td colspan="2"><u>FTP/TFTP Settings</u></td> </tr> <tr> <td>Hostname or IP Address of FTP/TFTP server</td> <td>100.10.20.1</td> </tr> <tr> <td>Username for FTP Server or Blank for TFTP Server</td> <td></td> </tr> <tr> <td>Password for FTP Server</td> <td></td> </tr> </table>		<u>FTP/TFTP Settings</u>		Hostname or IP Address of FTP/TFTP server	100.10.20.1	Username for FTP Server or Blank for TFTP Server		Password for FTP Server	
<u>FTP/TFTP Settings</u>									
Hostname or IP Address of FTP/TFTP server	100.10.20.1								
Username for FTP Server or Blank for TFTP Server									
Password for FTP Server									
<table border="1"> <tr> <td colspan="2"><u>Image Settings</u></td> </tr> <tr> <td>Image for Transfer</td> <td>image 1 ▼</td> </tr> <tr> <td>Image Filename (on server)</td> <td>1.5.0_OS.img</td> </tr> <tr> <td>Image Filename (on HTTP Client)</td> <td></td> </tr> </table>		<u>Image Settings</u>		Image for Transfer	image 1 ▼	Image Filename (on server)	1.5.0_OS.img	Image Filename (on HTTP Client)	
<u>Image Settings</u>									
Image for Transfer	image 1 ▼								
Image Filename (on server)	1.5.0_OS.img								
Image Filename (on HTTP Client)									
<div> <div>Get Image</div> <div>Put Image</div> </div> <div> <div>Browse...</div> <div>Download via Browser</div> </div>									

3. If you are loading software from your computer (HTTP client), go to step 4. If you are loading software from a FTP/TFTP server, enter the server's information in the FTP/TFTP Settings section.
4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
 - If you are loading software from a FTP/TFTP server, enter the file name and click Get Image.
 - If you are loading software from your computer, click Browse. In the File Upload Dialog, select the file and click OK. Click Download via Browser.

Once the image has loaded, the page refreshes to show the new software.

Using the AOS CLI

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

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

NOTE – The DNS parameters must be configured if specifying hostnames. See [“Domain Name System Configuration” on page 296](#).

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# gting
```

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 FTP or TFTP server.**

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

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

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

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

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

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

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 FTP or TFTP server.

1. **At the Boot Options# prompt, enter:**

```
Boot Options# ptimg
```

2. **The system prompts you for information. Enter the desired image:**

```
Enter name of switch software image to be uploaded  
["image1"|"image2"|"boot"]: <image>
```

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

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

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

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

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

```
image2 currently contains Software Version 1.3.0  
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.

Accessing the ISCLI

The default command-line interface for the GbESM is the Alteon OS CLI. To access the ISCLI, enter the following command and reset the GbESM:

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

To access the Alteon OS CLI, enter the following command from the ISCLI and reload the GbESM:

```
Router(config)# boot cli-mode aos
```

Users can select the CLI mode upon login, if the `/boot/prompt` command is enabled. Only an administrator connected through the console port can view and enable `/boot/prompt`. When `/boot/prompt` is enabled, the first user to log in can select the CLI mode. Subsequent users must use the selected CLI mode, until all users have logged out.

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    - Uencode FLASH dump
  ptdmp    - Upload FLASH dump via FTP/TFTP
  ptfile   - 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 (/maint)

Command Syntax and Usage

sys

Displays the System Maintenance Menu. To view menu options, see [page 346](#).

fdb

Displays the Forwarding Database Manipulation Menu. To view menu options, see [page 347](#).

debug

Displays the Debugging Menu. To view menu options, see [page 348](#).

Table 9-1 Maintenance Menu (/maint)

Command Syntax and Usage

arp

Displays the ARP Cache Manipulation Menu. To view menu options, see [page 349](#).

route

Displays the IP Route Manipulation Menu. To view menu options, see [page 350](#).

igmp

Displays the IGMP Maintenance Menu. To view menu options, see [page 351](#).

uudmp

Displays dump information in uuencoded format. For details, see [page 353](#).

ptdmp *<host name> <file name> [-mgmt | -data]*

Saves the system dump information via TFTP. For details, see [page 354](#).

ptfile

Uploads a specified file from switch the root file system to a FTP/TFTP server.

cldmp

Clears dump information from flash memory. For details, see [page 354](#).

panic

Dumps MP information to FLASH and reboots. For details, see [page 355](#).

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

This menu is reserved for use by IBM Service Support. The options are used to perform system debugging.

[System Maintenance Menu]	
flags	- Set NVRAM flag word
tmask	- Set MP trace mask word

Table 9-2 System Maintenance Menu Options (/maint/sys)

Command Syntax and Usage

flags	<i><new NVRAM flags word as 0XXXXXXXX></i>
This command sets the flags that are used for debugging purposes by Tech support group.	
tmask	<i><new trace mask word as 0XXXXXXXX></i> [p]
This command sets the trace mask that is used for debugging purposes by Tech support group.	

/maint/fdb

Forwarding Database Maintenance

[FDB Manipulation Menu]

- find - Show a single FDB entry by MAC address
- port - Show FDB entries for a single port
- trunk - Show FDB entries for a single trunk
- vlan - Show FDB entries for a single VLAN
- dump - Show all FDB entries
- clear - Clear entire FDB, then re-add static entries

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

Table 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 xxxxxxxxxxxxxx format (such as 080020123456).
port <port alias or number>	Displays all FDB entries for a particular port.
trunk <Trunk Group number>	Displays all FDB entries for a particular 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 77 .
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 Maintenance

```
[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 ARP Maintenance Menu Options (/maint/arp)

Command Syntax and Usage

find *<IP address (such as, 192.4.17.101)>*
Shows a single ARP entry by IP address.

port *<port alias or number>*
Shows ARP entries on a single port.

vlan *<VLAN number>*
Shows ARP entries on a single VLAN.

addr
Shows the list of IP addresses which the switch will respond to for ARP requests.

dump
Shows all ARP entries.

clear
Clears the entire ARP list from switch memory.

NOTE – To display all ARP entries currently held in the switch, or a portion according to one of the options listed on the menu above (find, port, vlan, dump), you can also refer to “ARP Information” on [page 98](#).

/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)

Command Syntax and Usage

find <IP address (such as, 192.4.17.101)>

Shows a single route by destination IP address.

gw <default gateway address (such as, 192.4.17.44)>

Shows routes to a default gateway.

type **indirect|direct|local|broadcast|martian|multicast**

Shows routes of a single type. For a description of IP routing types, see [Table 4-21 on page 96](#)

tag **fixed|static|addr|rip|ospf|bgp|broadcast|martian|multicast**

Shows routes of a single tag. For a description of IP routing tags, see [Table 4-22 on page 97](#)

if <interface number (1-128)>

Shows routes on a single interface.

dump

Shows all routes.

clear

Clears the route table from switch memory.

NOTE – To display all routes, you can also refer to “IP Routing Information” on [page 95](#).

/maint/igmp
IGMP Maintenance

[IGMP Multicast Group Menu]

group

- Multicast Group Menu

mrouter

- IGMP Multicast Router Port Menu

clear

- Clear group and mrouter tables

Table 9-7 describes the IGMP Maintenance commands.

Table 9-7 IGMP Maintenance Menu Options (/maint/igmp)

Command Syntax and Usage	
group	Displays the Multicast Group menu. To view menu options, see page 351 .
mrouter	Displays the Multicast Router Port menu. To view menu options, see page 352 .
clear	Clears the IGMP group table and Mrouter tables.

/maint/igmp/group
IGMP Group Maintenance

[IGMP Multicast Group Menu]

find

- Show a single group by IP group address

vlan

- Show groups on a single vlan

port

- Show groups on a single port

trunk

- Show groups on a single trunk

detail

- Show detail of a single group by IP address

dump

- Show all groups

clear

- Clear group tables

The following table describes the maintenance commands for IGMP multicast groups.

Table 9-8 IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage	
find <IP address>	Displays a single IGMP multicast group by its IP address.
vlan <VLAN number>	Displays all IGMP multicast groups on a single VLAN.

Table 9-8 IGMP Multicast Group Maintenance Menu Options (/maint/igmp/group)

Command Syntax and Usage	
port <Port number or alias>	Displays all IGMP multicast groups on a single port.
trunk <Trunk Group number>	Displays all IGMP multicast groups on a single trunk group.
detail <IP address>	Displays detailed information about a single IGMP multicast group.
dump	Displays information for all multicast groups.
clear	Clears the IGMP group tables.

/maint/igmp/mrouter
IGMP Multicast Routers Maintenance

[IGMP Multicast Routers Menu]	
vlan	- Show all multicast router ports on a single vlan
dump	- Show all multicast router ports
clear	- Clear multicast router port table

The following table describes the IGMP multicast router (Mrouter) maintenance commands.

Table 9-9 IGMP Mrouter Maintenance Menu Options (/maint/igmp/mrouter)

Command Syntax and Usage	
vlan <VLAN number>	Shows all IGMP multicast router ports on a single VLAN.
dump	Shows all multicast router ports.
clear	Clears the IGMP Multicast Router port table.

/maint/uudmp

Uencode Flash Dump

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

If you want to capture dump information to a file, set your communication software on your workstation to capture session data prior to issuing the `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 354](#).

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/cltmp

Clearing Dump Information

To clear dump information from flash memory, at the Maintenance# prompt, enter:

```
Maintenance# cltmp
```

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 Tue Mar 14, 2008:
Version 1.5.0 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 Tuesday March 14, 2008. 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>AOS<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>*], [*<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
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
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_putn: ABORTED
VRRP	Synchronization RX connection RESET.
VRRP	Synchronization RX connection TIMEOUT.
VRRP	Synchronization RX connection UNKNOWN CLOSE.
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
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 pre-emption 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
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
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> minutes 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 time-out"" ""logout"">"
PORT_MIRR	Port mirroring is enabled
PORT_MIRR	Port mirroring is disabled
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 time-out"" ""logout"">"
SSH	Server key autogen starts
SSH	Server key autogen completes
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.

Appendix B

Alteon OS SNMP Agent

The Alteon OS SNMP agent supports SNMP version 3. Security is provided through SNMP community strings. The default community strings are “public” for SNMP GET operation and “private” for SNMP SET operation. The community string can be modified only through the Command Line Interface (CLI). Alteon WebSystems is registered as Vendor 1872. Detailed SNMP MIBs and trap definitions of the Alteon OS SNMP agent are contained in the following Alteon OS enterprise MIB document:

GbESM-1G-2223.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:

- rfc1213.mib
- rfc1215.mib
- rfc1493.mib
- rfc1573.mib
- rfc1643.mib
- rfc1757.mib
- rfc1907.mib
- rfc2037.mib
- rfc2571.mib
- rfc2572.mib
- rfc2573.mib
- rfc2574.mib
- rfc2575.mib
- rfc2576.mib

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 9-10 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 9-10 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 9-11](#).

The examples in this section use the MIB name, but you can also use the OID.

[Table 9-11](#) lists the MIBs used to perform operations associated with the GbESM Switch Image and Configuration files. These MIBs are contained within in the file “aossswitch.mib”

Table 9-11 MIBs for Switch Image and Configuration Files

MIB Name	MIB OID
agTftpServer	1.3.6.1.4.1872.2.5.1.1.7.1.0
agTftpImage	1.3.6.1.4.1872.2.5.1.1.7.2.0
agTftpImageFileName	1.3.6.1.4.1872.2.5.1.1.7.3.0
agTftpCfgFileName	1.3.6.1.4.1872.2.5.1.1.7.4.0
agTftpDumpFileName	1.3.6.1.4.1872.2.5.1.1.7.5.0
agTftpAction	1.3.6.1.4.1872.2.5.1.1.7.6.0
agTftpLastActionStatus	1.3.6.1.4.1872.2.5.1.1.7.7.0
agTftpUserName	1.3.6.1.4.1872.2.5.1.1.7.9.0
agTftpPassword	1.3.6.1.4.1.1872.2.5.1.1.7.10.0
agTftpTSDumpFileName	1.3.6.1.4.1.1872.2.5.1.1.7.11.0

The following SNMP actions can be performed using the MIBs listed in [Table 9-11](#).

- Load a new Switch image (boot or running) from a FTP/TFTP server
- Load a previously saved switch configuration from a FTP/TFTP server
- Save the switch configuration to a FTP/TFTP server
- Save a switch dump to a FTP/TFTP server

Loading a new switch image

To load a new switch image with the name “MyNewImage-1.img” into image2, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch image resides:

```
Set agTftpServer.0 "192.168.10.10"
```

2. Set the area where the new image will be loaded:

```
Set agTftpImage.0 "image2"
```

3. Set the name of the image:

```
Set agTftpImageFileName.0 "MyNewImage-1.img"
```

4. Initiate the transfer. To transfer a switch image, enter 2 (gting):

```
Set agTftpAction.0 "2"
```

5. If you are using an FTP server, enter a username:

```
Set agTftpUserName.0 "MyName"
```

6. If you are using an FTP server, enter a password:

```
Set agTftpPassword.0 "MyPassword"
```

Loading a saved switch configuration

To load a saved switch configuration with the name “MyRunningConfig.cfg” into the switch, follow the steps below. This example assumes you have a TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the switch Configuration File resides:

```
Set agTftpServer.0 "192.168.10.10"
```

2. Set the name of the configuration file:

```
Set agTftpCfgFileName.0 "MyRunningConfig.cfg"
```

3. Initiate the transfer. To restore a running configuration, enter 3:

```
Set agTftpAction.0 "3"
```

4. If you are using an FTP server, enter a username:

```
Set agTftpUserName.0 "MyName"
```

5. If you are using an FTP server, enter a password:

```
Set agTftpPassword.0 "MyPassword"
```

Saving the switch configuration

To save the switch configuration to a FTP/TFTP server follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. Set the FTP/TFTP server address where the configuration file is saved:

```
Set agTftpServer.0 "192.168.10.10"
```

2. Set the name of the configuration file:

```
Set agTftpCfgFileName.0 "MyRunningConfig.cfg"
```

3. Initiate the transfer. To save a running configuration file, enter 4:

```
Set agTftpAction.0 "4"
```

4. If you are using an FTP server, enter a username:

```
Set agTftpUserName.0 "MyName"
```

5. If you are using an FTP server, enter a password:

```
Set agTftpPassword.0 "MyPassword"
```

Saving a switch dump

To save a switch dump to a FTP/TFTP server, follow the steps below. This example assumes you have a FTP/TFTP server at 192.168.10.10.

1. **Set the FTP/TFTP server address where the configuration will be saved:**

```
Set agTftpServer.0 "192.168.10.10"
```

2. **Set the name of dump file:**

```
Set agTftpDumpFileName.0 "MyDumpFile.dmp"
```

3. **Initiate the transfer. To save a dump file, enter 5:**

```
Set agTftpAction.0 "5"
```

4. **If you are using an FTP server, enter a username:**

```
Set agTftpUserName.0 "MyName"
```

5. **If you are using an FTP server, enter a password:**

```
Set agTftpPassword.0 "MyPassword"
```


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.
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.)
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	<p>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:</p> <ul style="list-style-type: none">■ 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 1024 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 standard VRRP MAC address as defined in the RFC is 00-00-5E-00-01-{VRID}. For virtual routers with a VRID greater than 255, the following block of MAC addresses is allocated: 00:0F:6A:9A:40:00 - 00:0F:6A:9A:47:FF

If you have a VRRP address shared between two switches, then the VRID must be identical on both switches so each virtual router on each switch knows with whom to share.

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.

Index

Symbols

/ command.....	50
[].....	16

A

abbreviating commands (CLI)	54
access control	
user.....	203
ACL Port menu	210
ACL statistics	161, 162
active configuration block	173, 340
active IP interface.....	305
active port	
VLAN	305
active switch configuration	
gtcfg	322
ptcfg	322
restoring	322
active switch, saving and loading configuration....	322
addr	
IP route tag	97
administrator account.....	27, 32
admpw (system option)	203
aging	
STP bridge option	233
STP information	83, 86
apply (global command).....	172
applying configuration changes.....	172
autoconfiguration	
link	37
auto-negotiation	
enable/disable on port.....	209
setup	37
autonomous system filter action.....	266

autonomous system filter path	
action	266
as	266
aspath	266

B

backup configuration block.....	173, 340
Bandwidth Management.....	251
banner (system option)	176
BBI	19
BGP	
configuration	280
eBGP.....	280
filters, aggregation configuration.....	285
iBGP	280
in route	283
IP address, border router	282
IP route tag.....	97
keep-alive time	282
peer	280
peer configuration	282
redistribution configuration	284
remote autonomous system.....	282
router hops	283
BLOCKING (port state)	84
boot options menu	333
bootstrap protocol	297
Border Gateway Protocol	97
configuration	280
Border Gateway Protocol (BGP)	
operations-level options	329
BPDU. <i>See</i> Bridge Protocol Data Unit.	
bridge parameter menu, for STP.....	230
bridge priority	83, 89
Bridge Protocol Data Unit (BPDU)	83, 89
STP transmission frequency	232
Bridge Spanning-Tree parameters	232

broadcast	
IP route tag	97
IP route type	96
Browser-Based Interface	19

C

capture dump information to a file	353
Cisco Ether Channel	238
CIST information	88
clear	
ARP entries	349
dump information	354
FDB entry	347
routing table	350
command (help)	50
Command-Line Interface (CLI)	19 to 29, 32, 47
commands	
abbreviations	54
conventions used in this manual	16
global commands	50
shortcuts	54
stacking	54
tab completion	54
configuration	
802.1x	218
administrator password	203
apply changes	172
CIST	226
default gateway interval, for health checks	255
default gateway IP address	255
dump command	321
failover	243
flow control	209
Gigabit Ethernet	207
IGMP	286
IP static route	257, 258
LDAP	184
operating mode	209
port link speed	209
port mirroring	319
port trunking	238
RIP	267
save changes	173
setup	321
setup command	321
SNMP	187
switch IP address	254
TACACS+	181
user password	203
view changes	172
VLAN default (PVID)	207
VLAN IP interface	254
VLAN tagging	207
VRRP	298
configuration block	
active	340
backup	340
factory	340
selection	340
configuration menu	169
configuring routing information protocol	268
connecting	
via console	20
console port	
connecting	20
COS queue information	115
cost	
STP information	84, 86, 90
STP port option	234
CPU statistics	160
CPU utilization	160
cur (system option)	180, 186, 201

D

date	
setup	35
system option	175
daylight savings time	175
debugging	343
default gateway	
information	94
interval, for health checks	255
default password	27
designated port	99
diff (global) command, viewing changes	172
direct (IP route type)	96
directed broadcasts	261
DISABLED (port state)	84
disconnect idle timeout	29
DNS statistics	143
downloading software	335
dump	
configuration command	321
maintenance	343
state information	355
duplex mode	
link status	56, 117
dynamic routes	350

E

End-to-End flow control	176
EtherChannel	
as used with port trunking	238

F

factory configuration block	340
factory default configuration	28, 32, 33
failover	
configuration	243
FDB statistics	135
Final Steps	41
first-time configuration	28, 31 to 46
fixed	
IP route tag	97
flag field	99
flow control	56, 117
configuring	209
setup	36

forwarding configuration	261
IP forwarding configuration	261
forwarding database (FDB)	343
Forwarding Database Information Menu	76
Forwarding Database Menu	347
forwarding state (FWD)	77, 83, 89, 91
fwd (STP bridge option)	233
FwdDel (forward delay), bridge port	83, 86, 89

G

gig (Port Menu option)	207
Gigabit Ethernet	
configuration	207
Gigabit Ethernet Physical Link	207
global commands	50
gtcfg (TFTP load command)	322

H

health checks	
default gateway interval, retries	255
retry, number of failed health checks	255
hello	
STP information	83, 86, 89
help	50
hot-standby failover	303
hprompt	
system option	176
HTTPS	206

I

ICMP statistics	143
idle timeout	
overview	29
IEEE 802.1s	85
IEEE 802.1w	85
IEEE standards	
802.1d	83, 230
802.1s	224
802.1w	224
802.1x	80
IGMP Snooping	287
IGMP statistics	149
image	
downloading	335
software, selecting	338
indirect (IP route type)	96

Information	
IGMP Information	110
IGMP Multicast Router Information	111
Trunk Group Information	91
information	
802.1p	114
Information Menu	55
Ingress Back Pressure (IBP) flow control	176
Interface change stats	154
IP address	39
ARP information	98
configuring default gateway	255
IP interface	39
IP configuration via setup	39
IP forwarding	
directed broadcasts	261
IP forwarding information	94
IP Information	109
IP Information Menu	94
IP interface	254
active	305
configuring address	254
configuring VLANs	254
IP interfaces	39, 96
information	94
IP route tag	97
priority increment value (ifs) for VRRP	307
IP network filter configuration	262
IP Route Manipulation Menu	350
IP routing	39
tag parameters	97
IP Static Route Menu	257, 258
IP statistics	140
IP subnet mask	39
IP switch processor statistics	137

L

LACP	241
Layer 2 Menu	74
Layer 3 Menu	93
LEARNING (port state)	83, 84, 89
link	
speed, configuring	209
Link Aggregation Control Protocol	241
link status	56
command	117
duplex mode	56, 117
port speed	56, 117

Link Status Information	117
linkt (SNMP option)	188
LISTENING (port state)	84
lmask (routing option)	94
lnet (routing option)	94
local (IP route type)	96
log	
syslog messages	177

M

MAC (media access control) address ..	58, 70, 76, 98, 347
Main Menu	48
Command-Line Interface (CLI)	28
summary	49
Maintenance	
IGMP	351
IGMP Groups	351
IGMP Multicast Routers	352
Maintenance Menu	343
management module	20
Management Processor (MP)	348
display MAC address	58, 70
manual style conventions	16
martian	
IP route tag (filtered)	97
IP route type (filtered out)	96
mask	
IP interface subnet address	254
mation	91
MaxAge (STP information)	83, 86, 89
MD5 cryptographic authentication	272
MD5 key	275
media access control. <i>See</i> MAC address.	
meter	
ACL	211
Miscellaneous Debug Menu	348
monitor port	319
mp	
packet	158
MP. <i>See</i> Management Processor.	
multicast	
IP route type	96
multiple management VLANs	247
Multiple Spanning Tree	
configuration	224
mxage (STP bridge option)	232

N

nbr change statistics.....	153
network management.....	19
notice.....	175
NTP server menu.....	186
NTP synchronization.....	186

O

online help.....	50
operating mode, configuring.....	209
operations menu.....	323
operations-level BGP options.....	329
operations-level IP options.....	329
Operations-Level Port Options.....	326, 327, 330
operations-level VRRP options.....	328
ospf	
area index.....	270, 272
authentication key.....	275
configuration.....	270
cost of the selected path.....	274
cost value of the host.....	277
dead, declaring a silent router to be down.....	275
dead, health parameter of a hello packet.....	276
export.....	278
fixed routes.....	280
general.....	151
global.....	151
hello, authentication parameter of a hello packet...	

276

host entry configuration.....	277
host routes.....	270
interface.....	270
interface configuration.....	274
link state database.....	270
Not-So-Stubby Area.....	272
priority value of the switch interface.....	274
range number.....	270
redistribution menu.....	270
route redistribution configuration.....	278
spf, shortest path first.....	272
stub area.....	272
summary range configuration.....	273
transit area.....	272
transit delay.....	275
type.....	272
virtual link.....	270
virtual link configuration.....	276
virtual neighbor, router ID.....	276
OSPF Database Information.....	104
OSPF general.....	102
OSPF General Information.....	103
OSPF Information.....	102
OSPF Information Route Codes.....	106
OSPF statistics.....	150

P

panic	
command.....	355
switch (and Maintenance Menu option).....	344
parameters	
tag.....	97
type.....	96
Password	
user access control.....	203
password	
administrator account.....	27
default.....	27
user account.....	27
VRRP authentication.....	306
passwords.....	27
ping.....	51
poisoned reverse, as used with split horizon.....	268
port configuration.....	207
port flow control. <i>See</i> flow control.	

Port Menu	
configuration options	207
configuring Gigabit Ethernet (gig)	207
port mirroring	
configuration	319
Port number	117
port speed	56, 117
port states	
UNK (unknown)	77
port trunking	
description	238
port trunking configuration	238
ports	
configuration	36
disabling (temporarily)	210
information	118
IP status	94
membership of the VLAN	75, 92
priority	83, 89
STP port priority	234
VLAN ID	57, 118
preemption	
assuming VRRP master routing authority	302
virtual router	301, 304
priority	
virtual router	304
priority (STP port option)	234
prisrv	
primary radius server	179
Private VLAN	250
Protected Mode	330
ptcfg (TFTP save command)	322
PVID (port VLAN ID)	57, 118
PVLAN	248
pwd	51

Q

quiet (screen display option)	51
-------------------------------------	----

R

RADIUS server menu	179
--------------------------	-----

read community string (SNMP option)	188
reboot	344, 355
receive flow control	36, 209
reference ports	77
referenced port	99
re-mark	212
restarting switch setup	34
retries	
radius server	179
retry	
health checks for default gateway	255
rip	
IP route tag	97
RIP Information	108
RIP information	107
RIP. <i>See</i> Routing Information Protocol.	
route statistics	142
router hops	283
routing information protocol	
configuration	268
Routing Information Protocol (RIP)	97
options	268
poisoned reverse	268
split horizon	268
version 1 parameters	267, 268
RSTP information	85
rx flow control	36
Rx/Tx statistics	152

S

save (global command)	173
noback option	173
save command	340
secret	
radius server	179
secsrv	
secondary radius server	179
Secure Shell	178
setup	
configuration	321
setup command, configuration	321

setup facility	28, 31	statistics	
IP configuration	39	management processor	157
IP subnet mask	39	Statistics Menu	121
port auto-negotiation mode	37	stopping switch setup	34
port configuration	36	subnet address maskconfiguration	
port flow control	36	IP subnet address	254
restarting	34	subnet mask	39
Spanning-Tree Protocol	36	subnets	39
starting	32	IP interface	254
stopping	34	switch	
system date	35	name and location	58, 70
system time	35	resetting	341
VLAN name	38	syslog	
VLAN tagging	37	system host log configuration	177
VLANs	38	system	
shortcuts (CLI)	54	contact (SNMP option)	188
snap traces		date and time	58, 70
buffer	348	information	70
SNMP	19, 122	location (SNMP option)	188
menu options	188	System Information	58
set and get access	188	System Maintenance Menu	346
SNMP Agent	369	system options	
SNMP statistics	163	admpw (administrator password)	203
SNMPv3	189	cur (current system parameters)	180, 186, 201
software		date	175
image	335	hprompt	176
image file and version	58, 71	login banner	176
spanning tree		time	175
configuration	230	tnport	201
Spanning-Tree Protocol	91	usrpw (user password)	203
bridge aging option	233	wport	200
bridge parameters	232	system parameters, current	180, 186, 201
bridge priority	83, 89		
port cost option	234	T	
port priority option	234	tab completion (CLI)	54
root bridge	83, 89, 232	tacacs	181
setup (on/off)	36	TACACS+	181
switch reset effect	341	TCP	138
split horizon	268	TCP statistics	146, 159
stacking commands (CLI)	54	Telnet	
starting switch setup	32	configuring switches using	321
state (STP information)	84, 86, 90	Telnet support	
static		optional setup for Telnet support	42
IP route tag	97	text conventions	16
static route		TFTP	337
rem	257	PUT and GET commands	322
statis route		TFTP server	322
add	257	thash	239

time	
setup	35
system option	175
timeout	
radius server	180
timeouts	
idle connection	29
timers kickoff	154
tnport	
system option	201
trace buffer	348
traceroute	51
Tracking	
VRRP	300
transmit flow control	36, 209
Trunk Group Information.....	91
trunk hash algorithm.....	239
tx flow control	36
type of area	
ospf	272
type parameters.....	96
typographic conventions, manual	16

U

UCB statistics	159
UDP	138
UDP statistics	148
unknown (UNK) port state	77
Unscheduled System Dump.....	355
upgrade, switch software.....	335
user access control configuration	203
user account.....	27
usrpw (system option).....	203
Uuencode Flash Dump.....	353

V

verbose	51
virtual router	
description.....	300
priority	304
tracking criteria	302
virtual router group	
VRRP priority tracking.....	303
virtual router group configuration	303
virtual router group priority tracking	305

Virtual Router Redundancy Protocol (VRRP)	
authentication parameters for IP interfaces	306
group options (prio).....	304
operations-level options	328
password, authentication	306
priority election for the virtual router	301
priority tracking options.....	282, 302
Virtual Router Redundancy Protocol configuration	298
virtual routers	
increasing priority level of.....	302
master preemption (preem).....	304
master preemption (prio).....	301
priority increment values (vrs) for VRRP	307
VLAN	
active port	305
configuration	246
VLAN tagging	
port configuration	207
port restrictions	247
setup	37
VLANs.....	39
ARP entry information	98
information	92
interface.....	40
name	75, 92
name setup.....	38
port membership	75, 92
setting default number (PVID).....	207
setup	38
tagging	37, 57, 118, 247
VLAN Number.....	92
VRID (virtual router ID)	300, 303
VRRP	
interface configuration.....	306
master advertisements.....	301
tracking	300
tracking configuration.....	307
VRRP Information.....	113
VRRP master advertisements	
time interval	304
VRRP statistics	155

W

watchdog timer.....	344
weights	
setting virtual router priority values	307
wport.....	200
write community string (SNMP option)	188