

HP ProLiant BL e-Class C-GbE Interconnect Switch Command Line Interface Reference Guide



February 2003 (First Edition)
Part Number 322857-001

© 2003 Hewlett-Packard Development Company, L.P.

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

HP ProLiant BL e-Class C-GbE Interconnect Switch Command Line Interface Reference Guide

February 2003 (First Edition)
Part Number 322857-001

Contents

About This Guide

Technician Notes	ix
Where to Go for Additional Help	x
Telephone Numbers	x

Chapter 1

Overview

Introduction	1-1
Additional References	1-1
Before You Begin	1-1
Accessing the Switch Modules	1-2
Moving Between the Console Management Interfaces	1-3
Setting the Default Interface	1-4
Displaying the Default Interface	1-4
Using the CLI	1-4
Understanding Command Syntax Symbols	1-4
Understanding Common Parameter Definitions	1-6
Using Command Line Editing Keys	1-7
Executing a Command	1-8
Using Command Completion	1-9
Displaying Command History	1-10
Customizing the Command Prompt	1-11
Clearing the CLI Screen	1-11
Paging of Data Output	1-12
Configuring the Switch Modules	1-12

Chapter 2

Configuring the Switch Modules using the Command Line Interface

Overview	2-1
Saving Changes	2-1
Managing User Accounts	2-2
Adding a User Account	2-3
Deleting a User Account	2-4
Displaying User Account Information	2-4
Updating User Account Information	2-4
Configuring Remote Management IP Interface Settings	2-5
Setting the Remote Management IP Interface Settings	2-6
Displaying Remote Management Interface Settings	2-8

Deleting the Secure IP Addresses.....	2-8
Configuring Basic Switch Module Information.....	2-9
Setting System Name, Location, and Contact Information	2-9
Displaying Switch Module Information	2-9
Configuring Auto-Logout Timer	2-13
Setting the Auto-Logout Time.....	2-13
Displaying Auto-Logout Timer Settings	2-14
Configuring MAC Address Aging Timer	2-14
Setting the MAC Address Age	2-15
Displaying MAC Address Aging Timer Information.....	2-15
Clearing MAC Address Monitoring Table	2-17
Configuring IGMP Snooping.....	2-18
Enabling IGMP Snooping	2-19
Disabling IGMP Snooping	2-20
Setting IGMP Filter Mode for Processing Multicast Packets.....	2-20
Adding IGMP Snooping Settings for a VLAN	2-21
Modifying IGMP Settings for a VLAN.....	2-22
Deleting IGMP Snooping Settings for a VLAN.....	2-23
Displaying IGMP Snooping Settings	2-23
Configuring Class of Service, Default Port Priority, and Traffic Class	2-25
Setting Class of Service, Default Port Priority, and Traffic Class.....	2-25
Displaying CoS Queue Information	2-27
Configuring Port Trunking	2-28
Considerations when Creating a Port Trunking Group	2-29
Creating a Port Trunk Group	2-30
Adding a Port to an Existing Trunk.....	2-30
Deleting a Trunk Group or a Port from a Trunk Group	2-31
Enabling a Trunk Group.....	2-31
Disabling a Trunk Group.....	2-31
Clearing Trunk Utilization Counters	2-31
Configuring the Trunk Load Sharing Algorithm Options	2-32
Displaying Trunk Load-Sharing Algorithm	2-32
Configuring GVRP	2-33
Enabling GVRP Globally or on a Per Port Basis	2-34
Disabling GVRP Globally or on a Per Port Basis	2-34
Displaying GVRP Settings	2-35
Configuring Telnet and Web Access Settings	2-35
Enabling Telnet Access	2-35
Disabling Telnet Access	2-35
Displaying Telnet Access Settings	2-36
Enabling Web Access.....	2-36
Disabling Web Access.....	2-36
Displaying Web Access Settings.....	2-36
Configuring Backpressure Flow Control	2-37
Enabling Backpressure Flow Control.....	2-37
Disabling Backpressure Flow Control.....	2-37
Displaying Backpressure Flow Control Settings.....	2-37
Configuring Switch Module Date and Time	2-38
Setting Date and Time Parameters Manually	2-39

Displaying Time Parameters.....	2-41
Enabling SNTP	2-41
Setting SNTP Parameters.....	2-42
Displaying SNTP Parameters	2-42
Disabling SNTP	2-43
Configuring Port Settings.....	2-43
Speed/Duplex Settings.....	2-43
Port Security Settings.....	2-44
Setting Port Parameters.....	2-45
Enabling Ports on a Per Port Basis	2-46
Disabling Ports or Port Security on a Per Port Basis	2-46
Clearing Current Port Statistics	2-46
Displaying Current Port Settings and Port Names.....	2-47
Configuring Bandwidth.....	2-49
Adding and Configuring Restart Port Bandwidth Units	2-49
Deleting Ports from the Ingress and Egress Bandwidth Tables.....	2-49
Modifying Ingress and Egress Bandwidth Parameters	2-50
Displaying Current and Restart Port Bandwidth Settings.....	2-50
Configuring Spanning Tree Protocol.....	2-51
Enabling STP	2-52
Disabling STP	2-53
Setting Global and Per Port STP Parameters	2-53
Displaying STP Bridging and Per Port Settings	2-56
Configuring Static (Destination Address) Filtering Table	2-57
Adding Unicast Filter Actions	2-57
Modifying Unicast Filter Actions	2-58
Deleting the Unicast Filter Actions.....	2-59
Displaying Unicast Filter Actions.....	2-59
Adding Multicast Filter Actions	2-60
Modifying Multicast Filter Actions	2-60
Deleting Multicast Filter Actions.....	2-61
Displaying Multicast Filter Settings for a VLAN.....	2-61
Configuring VLANs.....	2-62
Default VLAN	2-63
Creating an 802.1Q Static VLAN	2-64
Adding a Port to an Existing VLAN.....	2-65
Deleting a VLAN or a Port from an Existing VLAN	2-66
Modifying the Per Port VLAN Settings or VLAN Name.....	2-67
Setting the PVID for a Port.....	2-68
Displaying VLAN Settings and Status	2-69
Enabling Ingress Filtering on a Per Port Basis	2-70
Disabling Ingress Filtering on a Per Port Basis	2-70
Displaying Ingress Filtering Information.....	2-71
Configuring Port Mirroring	2-71
Enabling Mirroring on a Port.....	2-72
Disabling Mirroring on a Port.....	2-72
Displaying Port Mirroring Status.....	2-73
Configuring Thresholds for Broadcast, Multicast, DA-Unknown Storm Prevention or Monitoring.....	2-73
Enabling Broadcast, Multicast, or Unknown Packet Storm Monitoring	2-74

Disabling Monitoring Broadcast, Multicast, DA-Unknown Storm Monitoring.....	2-74
Configuring Storm Threshold in Packets Per Second	2-74
Displaying Broadcast, Multicast, DA-Unknown Storm Current Settings.....	2-75
Configuring Priority MAC Address.....	2-75
Adding Priority Level for a MAC Address	2-76
Deleting Priority Level for a MAC Address	2-76
Modifying Priority Level for a MAC Address	2-77
Displaying Current Priority Level for a MAC Address	2-77
Configuring the History Log.....	2-78
Displaying the History Log	2-78
Clearing the History Log.....	2-79
Configuring SNMP/RMON Manager.....	2-79
Adding SNMP Management Interface Community Strings.....	2-81
Deleting SNMP Management Interface Community Strings	2-82
Displaying Current SNMP Management Interface Settings.....	2-82
Using System Utilities	2-83
Setting TFTP	2-83
Initiating a TFTP Download for Firmware or Configuration File.....	2-84
Initiating a TFTP Upload for Log File or Configuration File	2-85
Displaying TFTP Parameters	2-86
Performing a Ping Test.....	2-87
Rebooting the Switch Module	2-87
Logging Out.....	2-87

Appendix A

Commands

Introduction.....	A-1
Using the Command Line Interface	A-1
Saving Changes.....	A-1
Managing User Accounts.....	A-2
Configuring Remote Management IP Interface Settings	A-2
Configuring Basic Switch Module Information.....	A-3
Configuring Auto-Logout Timer	A-3
Configuring MAC-Address Aging Timer.....	A-4
Configuring IGMP Snooping.....	A-5
Configuring Class of Service, Default Port Priority, and Traffic Class.....	A-6
Configuring Port Trunking	A-7
Configuring GVRP	A-8
Configuring Telnet and Web Access Settings	A-8
Configuring Backpressure Flow Control	A-8
Configuring Switch Module Date and Time.....	A-9
Enabling Simple Network Time Protocol (SNTP).....	A-10
Configuring Port Settings	A-11
Configuring Bandwidth	A-12
Configuring Spanning Tree Protocol	A-13
Configuring Static (Destination Address) Filtering Table	A-14
Configuring VLANs	A-15
Configuring Port Mirroring.....	A-16
Configuring Thresholds for Broadcast, Multicast, Unknown Storm Prevention or Monitoring	A-17

Configuring Priority MAC Address	A-17
Configuring the History Log	A-18
Configuring SNMP Manager	A-18
Using System Utilities	A-19
Rebooting the Switch Module	A-19
Logging Out	A-19

Index

About This Guide

This guide provides reference for configuring the interconnect switch through the command line interface (CLI).



WARNING: To reduce the risk of personal injury from electric shock and hazardous energy levels, only authorized service technicians should attempt to repair this equipment. Improper repairs can create conditions that are hazardous.

Technician Notes



WARNING: Only authorized technicians trained by HP should attempt to repair this equipment. All troubleshooting and repair procedures are detailed to allow only subassembly/module-level repair. Because of the complexity of the individual boards and subassemblies, no one should attempt to make repairs at the component level or to make modifications to any printed wiring board. Improper repairs can create a safety hazard.



WARNING: To reduce the risk of personal injury from electric shock and hazardous energy levels, do not exceed the level of repairs specified in these procedures. Because of the complexity of the individual boards and subassemblies, do not attempt to make repairs at the component level or to make modifications to any printed wiring board. Improper repairs can create conditions that are hazardous.



WARNING: To reduce the risk of electric shock or damage to the equipment:

- Disconnect power from the system by unplugging all power cords from the power supplies.
 - Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
 - Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
-



CAUTION: To properly ventilate the system, you must provide at least 7.6 cm (3.0 in.) of clearance at the front and back of the server.



CAUTION: The computer is designed to be electrically grounded (earthed). To ensure proper operation, plug the AC power cord into a properly grounded AC outlet only.

NOTE: Any indications of component replacement or printed wiring board modifications may void any warranty.

Where to Go for Additional Help

In addition to this guide, the following information sources are available:

- *HP ProLiant BL e-Class C-GbE Interconnect Switch User Guide*
- *HP ProLiant BL e-Class C-GbE Interconnect Switch Menu-driven Interface Reference Guide*
- *HP ProLiant BL e-Class C-GbE Interconnect Switch Web-based Interface Reference Guide*
- *Service Quick Reference Guide*
- Service training guides
- Service advisories and bulletins
- QuickFind information services
- Insight Manager software

Telephone Numbers

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.

For HP technical support:

- In the United States and Canada, call 1-800-652-6672.
- Outside the United States and Canada, refer to
www.hp.com

Introduction

The ProLiant BL e-Class C-GbE Interconnect Switch provides command line, menu-driven, Simple Network Management Protocol (SNMP), and Web-based management interfaces. The command line interface (CLI) and menu-driven interface allow you to set up and control the switch modules using either the serial or Ethernet ports on the switch. This guide discusses how to use the CLI to set up and manage the interconnect switch.

The command line interface provides standard scripting capabilities as well as enhanced systems management, monitoring, and deployment. The CLI can be accessed remotely via Telnet, or locally via the RS-232 console and SLIP sessions.

For quick reference, Appendix A provides a comprehensive listing of the commands supported by the command line interface.

Additional References

Additional information about installing and configuring the interconnect switch is available in the following guides, which are located on the ProLiant BL e-Class C-GbE Interconnect Switch Management System Utilities and User Documentation CD:

- *HP ProLiant BL e-Class C-GbE Interconnect Switch User Guide*
- *HP ProLiant BL e-Class C-GbE Interconnect Switch Menu-driven Interface Reference Guide*
- *HP ProLiant BL e-Class C-GbE Interconnect Switch Web-based Interface Reference Guide*

Before You Begin

The ProLiant BL e-Class C-GbE Interconnect Switch supports a wide array of functions and provides flexibility and increased network performance. Some planning is required to arrive at a deployment strategy that maximizes the potential of the interconnect switch. Refer to the “Planning the Interconnect Switch Configuration” section in *HP ProLiant e-Class C-GbE Interconnect Switch User Guide* for items to keep in mind as you configure your switch modules.

Accessing the Switch Modules

After the Integrated Administrator is configured, you can access and configure the switch modules through the Integrated Administrator software. For information on how to configure the Integrated Administrator, refer to the “Configuring the Integrated Administrator” section in the *HP ProLiant BL e-Class C-GbE Interconnect Switch User Guide*.

To access the switch modules from the Integrated Administrator command line interface, use one of the following methods:

- If you have already logged into the Integrated Administrator as the “Administrator,” you can connect to either switch module console using one of the following commands:

```
connect switch a to access Switch A
```

or

```
connect switch b to access Switch B
```

- If you have **not** logged on to the Integrated Administrator, you can use one of two special logon accounts to access the switch module consoles directly, depending on whether you want to access Switch A or Switch B. At the login prompt type in both the user name and password as either:

```
switcha
```

or

```
switchb
```

The logon screen for Switch A or Switch B will now be displayed.

```

      HP ProLiant BL e-Class C-GbE Interconnect Switch B
      Copyright(C)2001,2002 Hewlett-Packard Development Company, L.P

      Switch MAC: 00-02-A5-D1-02-95
      DUM IP: 192.168.2.76

      Username: [ ]
      Password: [ ]

                                                                 DISCONNECT
*****
Function:Enter case-sensitive username.
Message:
CTRL+R = Refresh
```

IMPORTANT: The interconnect switch does not have any initial user names or passwords set. HP recommends that after logging on, you create at least one Root-level user as the switch administrator. (Refer to Table 2-1 in Chapter 2 for an explanation of user privileges.) If you forget your password after it has been set up, call HP Customer Support to get a MAC-based backdoor password.

To log on for the first time:

1. Leave the **Username** field blank and press the **Tab** key.
2. Leave the **Password** field blank and press the **Enter** key. The main menu for the switch module is displayed.

NOTE: After user accounts are created, subsequent users will type their user name and password, then press the **Enter** key to gain access to the switch console.

```
ProLiant BL e-Class C-GbE Switch B Local Management
-----
Switch to CLI Mode
Configuration
Network Monitoring
SNMP Manager Configuration
User Accounts Management
System Utilities
Save Changes
Reboot
Logout

*****
Function:
Message:
For Help, press F1
```

The main menu displays the major categories for switch management.

Moving Between the Console Management Interfaces

The menu-driven interface is the factory default setting. To access the command line interface (CLI) from the menu-driven interface, highlight the **Switch to CLI Mode** option on the main menu and then press the **Enter** key. The command line prompt for the CLI will display.

```
>
```

When you are in a CLI session, you can access the menu-driven interface by executing the following command at the command prompt:

Command	Description
menu	Toggles from the CLI to the menu-driven interface

Moving between the CLI and menu-driven interface does not change the default interface. This means that if the default is the menu-driven interface and user 1 connects and switches to the CLI, when user 2 connects, they see the menu-driven interface when they log on.

Setting the Default Interface

Use the following command to change the interface default. This command takes effect immediately for the next log in. It will be lost however on reboot. To save the default permanently to non-volatile RAM (NVRAM), type the **cfg save** command. Refer to the “Saving Changes” section later in this chapter.

Use the following command to set the default interface:

Command	Description
def-interface set {menu cli}	Sets the default interface to either the menu-driven interface or the CLI

Displaying the Default Interface

Use the following command to display the default interface:

Command	Description
def-interface show	Displays the default interface

Using the CLI

This section describes how to use the command line interface to enter CLI commands.

Understanding Command Syntax Symbols

Command syntax is presented as a combination of defined strings, keywords, variables, and symbols. Symbols indicate how to enter the command, and should not be typed as part of the command itself.

Text in **boldface** must be entered literally as shown. Do not type any symbols that may appear in boldface.

The following table summarizes the command syntax symbols:

Table 1-1: Command Syntax Symbols

Symbol	Description	Example
<i><variable></i>	Angle brackets (< >) enclose italicized text. You must enter the correct variable or variables for the text.	user delete user <i><username></i> In this example, you type user delete user and the name of user account you want to delete.
[]	Square brackets ([]) enclose an optional entry.	system show [advanced] Acceptable entries are: <ul style="list-style-type: none"> system show system show advanced
	If several optional items are listed, the items may be entered in any order.	log show [num <i><num></i>] [item <i><index></i>] Acceptable entries are: <ul style="list-style-type: none"> log show log show num <i><num></i> log show item <i><index></i> log show num <i><num></i> item <i><index></i> log show item <i><index></i> num <i><num></i>
{ }	Curly brackets ({ }) enclose a required entry. If several optional items are listed inside curly brackets, you must type at least one of those items.	bandwidth delete port <i><portlist></i> { [ingress] [egress] } Acceptable entries are: <ul style="list-style-type: none"> bandwidth delete port <i><portlist></i> ingress bandwidth delete port <i><portlist></i> egress bandwidth delete port <i><portlist></i> ingress egress bandwidth delete port <i><portlist></i> egress ingress
	Vertical bars () separate mutually exclusive items in a list, of which exactly one may be typed.	igmp set filter {all unregistered filter} Acceptable entries are: <ul style="list-style-type: none"> igmp set filter all igmp set filter unregistered igmp set filter filter

Understanding Common Parameter Definitions

The following table describes how to enter common variable parameters used throughout this chapter.

Table 1-2: Common Parameters

Parameter	Description
<code><string></code>	<p>Type character strings as follows:</p> <ul style="list-style-type: none"> If the string of character includes blank space, you must type it within quotation marks (" "). Example: system set sysname "lab switch" If the string of characters does not include any blank space, you may type the string within or without quotation marks (" "). Example: system set sysname lab
<code><portlist></code>	<p>Type a port number or numbers in the following ways:</p> <ul style="list-style-type: none"> One number Example: port 3 A list of numbers are separated by a comma (,). Example: port 1, 3, 6, 8 A range of numbers are entered with a dash (-). Example: port 1-3 A range of numbers plus additional numbers are separated by commas Example: port 1-3, 6, 8 All ports are identified by adding an asterisk (*) after the keyword port Example: port *
<code><ip_addr></code>	<p>Type an IP address in the following format where xxx is a number from 0 to 255. Leading zeros may be used, but are not required.</p> <p>Format: xxx.xxx.xxx.xxx</p> <p>Example: 172.1.001.1</p>
<code><iplist></code>	<p>Type the IP address or addresses. Separate multiple IP addresses with commas.</p>
<code><mac_addr></code>	<p>Type a MAC address in the following format where xx is a two-digit, zero-filled, hexadecimal number.</p> <p>Format: xx.xx.xx.xx.xx.xx</p> <p>Example: 00.02.A5.D1.01.44</p>

continued

Table 1-2: Common Parameters *continued*

Parameter	Description
<code><vlan_id></code>	Type a VLAN ID in the following format where nnnn is a number from 1 to 4094. Leading zeros are allowed, but not necessary. Format: nnnn Example: 24
<code><vlan_name></code>	Type a name that is 1 to 15 characters in length to identify the VLAN. Use an underscore (_) to connect words. If the string of character includes blank space, you must type it within quotation marks (" "). Example: default_vlan
<code><vlanlist></code>	Type a VLAN number or numbers in the following ways: <ul style="list-style-type: none"> One number Example: vlan 20 A list of numbers are separated by a comma (,) Example: vlan 10, 30, 60, 80 A range of numbers are entered with a dash (-) Example: vlan 10-15 A range of numbers plus additional numbers are separated by commas Example: vlan 10-15, 60, 80 All VLANs on all units are identified by adding an asterisk (*) after the keyword vlan Example: vlan *

Using Command Line Editing Keys

The following describes the line-editing keys available using the CLI:

Keys	Description
Backspace	Deletes the character to the left of the cursor and shifts the remainder of the line to the left
Ctrl+D or Delete	Deletes the character under the cursor and shifts the remainder of the line to the left
Ctrl+F or Right Arrow	Moves the cursor to the right
Ctrl+B or Left Arrow	Moves the cursor to the left
Ctrl+A	Moves the cursor to the first character in the line
Ctrl+E	Moves the cursor to the space to the right of the last character in the line
Ctrl+C	Terminates the command and displays a new prompt

Executing a Command

Several help features are available to make executing commands easy.

Command Help

The help command can be used to display

- A complete list of all commands
- A description of a specific command, including valid parameters, their ranges, and the default

Command	Description
help	Displays a complete list of available commands
[<command>]	To display a help message for a specific command, type help and the command.

The following list displays when you type the command **help**.

```
Command: help
..
auto-logout set time-out
backpressure
bandwidth
bandwidth show
cfg show
cos set
def-interface set
dir
gvrp enable
help
igmp add
igmp disable
igmp modify vlan
igmp show
ingress-filtering enable port
log clear
login
mac-addr clear
mac-addr show
mac-pri delete
mac-pri show
mgmt-if delete secure-ip
?
auto-logout show
backpressure show
bandwidth delete port
cfg save
clear
cos show
def-interface show
gvrp disable
gvrp show
history
igmp delete vlan
igmp enable
igmp set filter
ingress-filtering disable port
ingress-filtering show
log show
logout
mac-addr set mac-age
mac-pri add
mac-pri modify
menu
CTRL+C [ESC] Quit [SPACE] Next Page [ENTER] Next Entry [A] All
```

The following displays when you type **help cos set**.

```
>help cos set
Command: help cos set

Command: cos set
Usage: cos set{sched !queue ! def-pri-tag tag ! pri-map pri }.
>_
```

Question Mark (?)

You can also access help by typing a question mark (?) at the beginning of a command or partial command.

This example shows the help that displays when you type **? gvrp enable**.

```
>? gvrp enable
Command: ? gvrp enable

Command: gvrp enable
Usage: gvrp enable {feature ! port <portlist>}
>
```

Using Command Completion

You can complete a command by typing a partial character string at the command prompt and then pressing the **Tab** key. When possible, the system displays the complete command for you. When not possible, the system generates an error message.

For example:

At the command prompt, type **sy sh** and then press the **Tab** key.

```
>sy sh_
```

The system completes the command.

```
>system show
```

The cursor appears immediately after the keyword, allowing you to enter additional information. If no command exists that matches what you have typed, no action is carried out and the system returns to the prompt.

In addition, you can type an abbreviation for the command and press the **Enter** key. The system will complete and execute your command if possible.

For example:

At the command prompt, type **sys sh** and then press the **Enter** key. The system completes and executes the command.

```
>system show
Command: system show
Device Type       : HP ProLiant BL e-Class C-GbE Interconnect Switch A
Option #         : 243283-B21
Switch Spare #    : 253077-001
MAC Address       : 00-02-A5-D1-06-40
Boot PROM Version : Build
Manufacturing Date: 04/29/02
Firmware Version  : 2.0.0
Build Date        : 21 Jan 2003-001
Hardware Version   : 2A1
Configuration Save Time: Unknown
System Up Time     : 0 days 00:25:57
Time              : Unknown
Time Source        : System Clock
System Name        :
System Location    :
System Contact     :
>_
```

Displaying Command History

The CLI maintains a buffer of recent commands that have been entered, with a maximum of 25 commands saved in the buffer per CLI session. When the buffer reaches 25 commands, it adds any new commands and deletes the earliest commands.

Use the following command to display the history buffer:

Command	Description
history	Displays the contents of the history buffer

Use the following to clear the commands in the history buffer:

Command	Description
history clear	Clears the history buffer

Customizing the Command Prompt

The default command prompt is the greater than sign (>). You can customize the command prompt using the following command:

Command	Description
prompt <prompt_string>	Customizes the command prompt Type prompt and the customized prompt word or string of words. The customized prompt takes effect immediately, for all sessions and all users.

For example:

```
>prompt John
Command: prompt "John"
John>_
```

Clearing the CLI Screen

To clear the current CLI screen and display a fresh page with a command prompt, use the following command:

Command	Description
clear	Clears the current CLI screen and displays a fresh page with a command prompt

Paging of Data Output

You can configure the switch module to display one page of data at a time. This is helpful when you are in a Telnet session and are using the show commands to display information about the switch module.

Paging is **on** with every new CLI session. To avoid the paging prompts when using scripts, set paging to **off**.

Use the following command to set the paging option:

Command	Description
paging {on off}	Configures the switch to display one page of data at a time If paging is turned off, data will display continuously until the end of the data is reached.

Configuring the Switch Modules

After logging on to the interconnect switch for the first time, perform the following tasks for each switch module:

1. Configure the IP address
2. Set up users, passwords, and access privileges
3. Change default SNMP community strings for read/write and read-only

For information on how to configure these and other interconnect switch features, refer to Chapter 2.

NOTE: After configuring the IP address on the switch module, the switch module can be accessed using Telnet, SNMP, or a Web browser. Refer to the section, “Configuring the Remote Management IP Interface Settings,” in Chapter 2 for information on how to set up the IP address.

Configuring the Switch Modules using the Command Line Interface

Overview

This chapter describes how to configure the switch modules from the command line interface (CLI).

Saving Changes

The switch module has two types of memory: dynamic RAM and non-volatile RAM (NVRAM).

Restarting the switch module erases all configuration settings in RAM and reloads the stored settings from NVRAM. Thus, it is necessary to save all configuration setting changes to NVRAM before rebooting the switch module.

After the configuration settings have been saved to NVRAM, they become the current runtime settings for the switch module. These settings are then used every time the switch module is rebooted.

Use the following command to retain any configuration changes permanently in NVRAM:

Command	Description
cfg save	Saves current configuration settings to the switch NVRAM

IMPORTANT: After saving your final configuration, HP highly recommends that you save the configuration image to TFTP server storage. Refer to the “Initiating a TFTP Upload for Log File or Configuration File” section later in this chapter for more information.

Use the following command to display the current configuration settings:

Command	Description
cfg show	Displays current configuration settings

For example:

```
Command: cfg show
<?xml version="1.0" encoding="UTF-8"?>
<SWITCH_CONFIG>
  <IP_ADDRESS>
    <GET_IP_FROM VALUE="DHCP"/>
    <IP_ADDRESS VALUE="192.168.2.85"/>
    <SUBNET_MASK VALUE="255.255.255.0"/>
    <DEFAULT_GATEWAY VALUE="192.168.2.251"/>
    <MANAGEMENT_VID VALUE="1"/>
  </IP_ADDRESS>
  <SYSTEM_INFORMATION>
    <NAME VALUE=""/>
    <LOCATION VALUE=""/>
    <CONTACT VALUE=""/>
  </SYSTEM_INFORMATION>
  <ADVANCED_SETTINGS>
    <TELNET_CONSOLE_AUTO_LOGOUT_IN_MINUTES VALUE="Never"/>
    <WEB_AUTO_LOGOUT_IN_MINUTES VALUE="5"/>
    <MAC_ADDRESS_AGING_TIME_IN_SECONDS VALUE="300"/>
    <IGMP_SNOOPING VALUE="Disabled"/>
    <GURP_STATUS VALUE="Disabled"/>
    <TELNET_STATUS VALUE="Enabled"/>
    <WEB_STATUS VALUE="Enabled"/>
  </ADVANCED_SETTINGS>
</SWITCH_CONFIG>

■ CTRL+C ■ ESC ■ Quit ■ SPACE ■ Next Page ■ ENTER Next Entry ■ All _
```

Managing User Accounts

After logging on to the switch module for the first time, you need to set up at least one user account with Root access rights. You can set up a maximum of eight users on a switch module.

There are three levels of user access rights: Root, User+, and User. Some menu selections available to users with Root privileges may not be available to those with User+ and User privileges.

The following table summarizes user access rights.

Table 2-1: User Access Rights

Privilege	Root	User+	User
Configuration	Yes	Read-only	Read-only
Network Monitoring	Yes	Read-only	Read-only
Community Strings and Trap Stations	Yes	Read-only	Read-only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Ping-only	Ping-only
Factory Reset	Yes	No	No
Reboot Switch	Yes	Yes	No
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	No	No

The following shows the factory default user account settings:

Feature	Default Value
Username	None
Password	None

Adding a User Account

Use the following command to add user account information:

Command	Description
user add	Adds a user account
user <username>	Type the following in the command:
access {r u+ u}	<ul style="list-style-type: none"> • user <username>—Type user and the user's name. Username can be between 1 and 15 characters. • access {r u+ u}—Type access and the user's access level: <ul style="list-style-type: none"> • r—root • u+—user + • u—user <p>After entering the command, the system will prompt twice to enter the user's password.</p>

Deleting a User Account

Use the following command to delete a user account:

Command	Description
user delete user <username>	Deletes the specified user's account

Displaying User Account Information

Use the following command to display user account information:

Command	Description
user show	Displays all user account information including each user's name and access level

For example:

```
>user show
Command: user show

Username                Access Level
-----                -
jane                    user
mike                    Root
>_
```

Updating User Account Information

Use the following command to modify user account information:

Command	Description
user modify user <username>	Modifies a user's account information
{	Type the user's name and one or both of the following:
[access {r u+ u}]	<ul style="list-style-type: none">• access {r u+ u}—Type access the new access level:
[password]	<ul style="list-style-type: none">• r—root• u+—user +• u—user
}	<ul style="list-style-type: none">• password—If password is entered, the system will prompt twice to enter the user's password.

Configuring Remote Management IP Interface Settings

Each switch module must be assigned its own IP address, which is used for communication with an SNMP network manager or other TCP/IP application (for example Web or TFTP). The factory default is set for the switch module to automatically obtain the IP address using DHCP service from a DHCP server on the attached network. You can also manually change the default switch IP address to meet the specification of your networking address scheme. If you select the manual mode and do not assign the IP address, the system assigns a default IP address for Switch A as 10.90.90.90 and for Switch B as 10.90.90.91. The system also assigns a default subnet mask of 255.0.0.0.

The switch module IP interface is also assigned a unique MAC address by the factory. This MAC address cannot be changed and can be found on the initial boot console screen and Logon screen, or by accessing basic switch information. Refer to the “Displaying Switch Module Information” section later in this chapter.

In addition, you can

- Set an IP address for a default gateway. This becomes necessary when the network management station is located on a different IP network from the switch module, making it necessary for management packets to go through a router to reach the network manager, and vice-versa.
- Set a list of up to eight secure IP addresses of network management stations that are allowed to manage the interconnect switch. Only those network management stations can access the switch management interfaces once set.
- Set a management VLAN ID (VID) for the IP interface so that the interconnect switch can be accessed from the designated management VLAN.
- Change the default SNMP community strings in the switch module and set the access rights of these community strings. Refer to the “Adding SNMP Management Interface Community Strings” section later in this chapter.

The following shows the factory default remote management settings:

Feature	Default Value
DHCP Service	Enabled
BootP Service	Disabled
IP Address (if DHCP is selected)	Switch A = DHCP server assigned unique IP address, subnet mask, and default gateway Switch B = DHCP server assigned unique IP address, subnet mask, and default gateway
IP Address (if manual IP option is selected)	Switch A = 10.90.90.90 Switch B = 10.90.90.91
Subnet Mask (if manual IP option is selected)	255.0.0.0
Default Gateway (if manual IP option is selected)	0.0.0.0
Management VID (MVID)	1

Setting the Remote Management IP Interface Settings

To access and manage the interconnect switch from an SNMP-based Network Management System, or by using the Telnet protocol or the Web, you must first configure the remote management IP interface parameters.

The IP address can be assigned by one of the following methods:

- **Manual**—This option allows you to manually configure an IP address, subnet mask, and default gateway for the switch module.
- **BOOTP**—This option configures the switch to send out a BOOTP broadcast request for IP information. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server attached to the same network to which the interconnect switch is connected.
- **DHCP**—This option configures the switch to send out a DHCP broadcast request. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server attached to the same network to which the interconnect switch is connected. DHCP protocol is the factory default mode.

Use the following command to configure the remote management IP interface settings:

Command	Description
<pre> mgmt-if set { [mode {manual bootp dhcp}] [ipaddr <ip_addr>] [netmask <subnet_mask>] [def-gateway <ip_addr>] [mvid <vlan_id>] [secure-ip <iplist>] } </pre>	<p>Sets the remote management parameters including:</p> <ul style="list-style-type: none"> • mode {manual bootp dhcp}—Type mode and manual, bootp, or dhcp. The default is dhcp. <p>If you choose manual, type the following:</p> <ul style="list-style-type: none"> • ipaddr <ip_addr>—Type ipaddr and the IP address in the form of <i>xxx.xxx.xxx.xxx</i>, where each <i>xxx</i> is a number between 0 and 255. • netmask <subnet_mask>—Type netmask and 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, 255.255.255.0 for a Class C network, or type a custom subnet mask. • def_gateway <ip_addr>—Type def-gateway and the IP address that determines where packets with a destination address outside the current subnet should be sent. • mvid <vlan_id>—Management VLAN ID (MVID) is the VLAN ID of the management processor port. Type mvid and the VLAN ID through which you want to access the switch module management interface. • secure-ip <iplist>—Type secure-ip and the management station IP addresses that are allowed to access the switch management interface. Enter from one to eight addresses, separated by commas.

Displaying Remote Management Interface Settings

Use the following command to display the remote management interface settings:

Command	Description
mgmt-if show	Displays the remote management interface current IP and VLAN settings

For example:

```
>mgmt-if show
Command: mgmt-if show

Get IP From      : DHCP
IP address       : 192.168.2.85
subnet Mask      : 255.255.255.0
Default Gateway  : 192.168.2.251
Management UID   : 1
Management Stations

IP Address
-----
>_
```

Deleting the Secure IP Addresses

Use the following command to delete the secure IP addresses:

Command	Description
mgmt-if delete secure-ip <iplist>	Deletes the secure IP addresses
	Enter from one to eight addresses, separated by commas.

Configuring Basic Switch Module Information

This section describes how to configure basic switch information.

Setting System Name, Location, and Contact Information

The following shows the factory default settings for system name, system location, and system contact:

Feature	Default Value
System Name	None
System Location	None
System Contact	None

Use the following command to configure the system name, location, and contact information:

Command	Description
system set <pre>{ [sysname <system_name>] [sysloc <system_location>] [contact <system_contact >] }</pre>	<p>Configures system information</p> <p>Enter the following in the command:</p> <ul style="list-style-type: none"> • sysname <system_name>—Type sysname and a system name. The system name can be up to 255 characters in length. Blank spaces are allowed. • sysloc <system_location>—Type sysloc and the system location. The system location can be up to 255 characters in length. Blank spaces are allowed. • contact <system_contact >—Type contact and the name of the contact person. HP recommends entering the name of the person who is responsible for the maintenance of the network system on which the switch module is located. The contact name can be up to 255 characters in length. White spaces are allowed.

Displaying Switch Module Information

You can display basic information about the switch module including the type of switch and the MAC address (assigned by the factory and unchangeable) for that switch module. In addition, the boot PROM and firmware version numbers display. This information is helpful in monitoring PROM and firmware updates.

You can also display the settings for the advanced switch features including global settings for IGMP snooping, GVRP, Telnet status, Web status, SNMP, and others.

Use the following command to display the switch module information:

Command	Description
system show	Displays basic switch information
[advanced]	Type advanced in the command to display advanced switch information. Refer to the following examples.

This example shows the basic switch information.

```
>system show
Command: system show
Device Type       : HP ProLiant BL e-Class C-GbE Interconnect Switch A
Option #         : 243283-B21
Switch Spare #    : 253077-001
MAC Address       : 00-02-A5-D1-06-40
Boot PROM Version : Build
Manufacturing Date: 04/29/02
Firmware Version  : 2.0.0
Build Date        : 21 Jan 2003-001
Hardware Version  : 2A1
Configuration Save Time: Unknown
System Up Time    : 0 days 00:25:57
Time              : Unknown
Time Source       : System Clock
System Name       :
System Location    :
System Contact     :
>_
```

- **Device Type**—Displays the name of the switch module.
- **Option #**—Displays the option number for the switch module and Interconnect Module combination.
- **Switch Spare #**—Displays the spare part number for the switch module.
- **MAC Address**—Identifies the Ethernet address for the switch module.
- **Boot PROM Version**—Identifies the version number of Boot PROM code installed on the interconnect switch.
- **Manufacturing Date**—Displays the manufacture date of the switch module.
- **Firmware Version**—Identifies the version number of the firmware installed on the switch module.
- **Build Date**—Displays the firmware build date number.
- **Hardware Version**—Identifies the version number of the interconnect switch hardware build.
- **Configuration Save Time**—Displays the time the current settings were saved to the configuration file. If the current time has never been set up on the interconnect switch, “Unknown” will be displayed.

- **System Up Time**—Identifies the time the switch booted up, if the current time has been set on the switch module. If the current time has never been set up on the interconnect switch, this field identifies the time since the switch module was booted up.
- **Time**—Displays the current real time set on the switch module. If the current time has never been set up on the interconnect switch, “Unknown” will be displayed.
- **Time Source**—Displays how the switch module obtains the current time: Primary SNTP Server, Secondary SNTP Server, or System Clock.
- **System Name**—Displays a user-configured name for the switch module.
- **System Location**—Displays a user-configured description for the physical location of the switch module.
- **System Contact**—Displays the user-configured name of the person to contact if there are any problems or questions with the switch module.

This example shows the advanced switch features.

```
>system show advanced
Command: system show advanced

Auto-Logout                  : 10 mins
MAC Address Aging Time      : 300 sec
IGMP Snooping Status        : Disabled
Switch GURP                 : Disabled
Telnet Status               : Enabled
Web Status                  : Enabled
Group Address Filter Mode   : Forward All Unregistered
Scheduling Mechanism for CoS Queues : Strict
Trunk Load Sharing Algorithm : Src Address
Backpressure                : Disabled
TFIP Port Number           : 69
SNTP Status                 : Disabled
SNTP Server1 IP             : 0.0.0.0
SNTP Server2 IP            : 0.0.0.0
SNTP Poll Interval         : 64 Sec.
Time Zone                   : -6:0
Daylight Saving Time State   : Disabled
Daylight Saving Time Start   Month : April      Week : 1st Week   Day : Sunday
Daylight Saving Time End    Month : October    Week : Last One   Day : Sunday
>
```

- **Auto Logout**—Displays the time that the RS-232 console and Telnet management interface can be idle before the switch module automatically logs out the user. For additional information, refer to the “Configuring Auto-Logout Timer” section later in this chapter.
- **MAC Address Aging Time**—Displays the length of time a learned MAC address remains in the forwarding table without being seen as a source (that is, how long a learned MAC address is allowed to remain idle before being deleted from the address table). For additional information, refer to the “Configuring MAC Address Aging Timer” section later in this chapter.
- **IGMP Snooping Status**—Displays the Internet Group Management Protocol (IGMP) snooping status set on the switch module. IGMP snooping enables the switch module to register IGMP packets being forwarded through the switch module in order to obtain multicast member information from them, such as which ports are attached to which multicst members. For additional information, refer to the “Configuring IGMP Snooping” section later in this chapter.

- **Switch GVRP Status**— Displays the GARP VLAN Registration Protocol (GVRP) status set on the interconnect switch. GVRP allows dynamic propagation of VLAN registration information across the GVRP-enabled switches on the same network. For additional information, refer to the “Configuring GVRP” section later in this chapter.
- **Telnet Status**—Displays the Telnet status set on the switch module. This setting enables or disables access to the switch module over the network using the Telnet protocol. For additional information, refer to the “Configuring Telnet and Web Access Settings” section later in this chapter.
- **Web Status**—Displays the Web status set on the switch module. This setting enables or disables management of the switch module over the Web. For additional information, refer to the “Configuring Telnet and Web Access Settings” section later in this chapter.
- **Group Address Filter Mode**—Displays the IGMP group address filter mode for forwarding multicast packets. For additional information, refer to the “Configuring IGMP Snooping, section later in this chapter. For additional information, refer to the “Configuring Telnet and Web Access Settings” section later in this chapter.
- **Scheduling Mechanism for CoS Queues**—Displays the Class of Service queue scheduling option set on the switch module. For additional information, refer to the “Configuring Class of Service, Default Port Priority, and Traffic Class” section later in this chapter.
- **Trunk Load Sharing Algorithm**—Displays the port trunk load sharing option set on the switch module. This setting determines if load balancing decisions will be made based on the source MAC address, destination MAC address, or both addresses. For additional information, refer to the “Configuring the Trunk Load Sharing Algorithm Options” later in this chapter.
- **Backpressure**— Displays the backpressure option set on the 10/100 ports of the switch module. When backpressure is enabled and there is incoming traffic congestion on a 10/100 port, the receiving port sends a request to the transmitting port. The transmitting port acknowledges the request and stops sending packets for a random amount of time, before it starts sending again. For additional information, refer to the “Configuring Backpressure Flow Control” section later in this chapter.
- **TFTP Port Number**—Displays the port number used for the TFTP server. For additional information, refer to the “Using System Utilities” section later in this chapter.
- **SNTP Status**—Displays the Simple Network Time Protocol (SNTP) status set on the switch. SNTP allows the switch to synchronize its real time to the network time. When SNTP is enabled, the interconnect switch sends a request to a primary SNTP server in each period of a specified polling interval asking for the Greenwich Mean Time (GMT). If the primary SNTP server is not available, the request is sent to a secondary SNTP server. For additional information, refer to the “Configuring Switch Module Date and Time” section later in this chapter.
- **SNTP Server1 IP**—Displays the IP address for the primary SNTP server the switch module can use.
- **SNTP Server2 IP**—Displays the IP address for the secondary SNTP server the switch module can use.

- **SNTP Poll Interval**—Displays the polling interval set on the switch module to synchronize with the network time.
- **Time Zone**—Displays the number of hours and minutes that the time zone is ahead (+) or behind (-) Greenwich Mean Time (GMT).
- **Daylight Saving Time State**—Displays if daylight saving time settings are enabled or disabled on the switch module.
- **Daylight Saving Time Start Month, Week, Day**—Displays the month, week, and day that daylight saving time is set to start.
- **Daylight Saving Time End Month, Week, Day**—Displays the month, week, and day that daylight saving time is set to end.

Configuring Auto-Logout Timer

The auto-logout timer sets the time the RS-232 console and Telnet management interfaces can be idle before the switch module automatically logs out the user.

The following shows the factory default setting for the auto-logout timer:

Feature	Default Value
Auto Logout	10 minutes

Setting the Auto-Logout Time

Use the following command to set the auto-logout time:

Command	Description
auto-logout set time-out {0 2 5 10 15}	Sets the auto-logout timer for idle timeout of the RS-232 console and Telnet management interface sessions. The options are: 0 , 2 , 5 , 10 , and 15 minutes. Zero (0) indicates never timing out.

Displaying Auto-Logout Timer Settings

Use the following command to show the auto-logout timer settings:

Command	Description
auto-logout show	Displays the current value set for the auto-logout timer for idle timeout of the RS-232 console and Telnet management interface sessions

For example:

```
>auto-logout show
Command: auto-logout show
Auto-Logout : 10 mins
>_
```

Configuring MAC Address Aging Timer

The switch module enters into its forwarding table the mapping between the MAC address of the device and the Ethernet port to which the device is attached. This information is used to forward packets. This reduces the traffic congestion on the network, because packets are forwarded to the destination port only, instead of being forwarded to all ports.

The MAC address aging timer prunes the forwarding table addresses entries that are no longer used. Dynamic forwarding table entries, which are made up of MAC addresses and their associated port numbers, are deleted from the table if they are not seen within the aging timeout. The aging time can be from 10 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer are used.

If the aging time is too short, however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table. In this case the switch module will send the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

The following shows the factory default setting for the MAC address aging time:

Feature	Default Value
MAC Address Aging Time	300 seconds

Setting the MAC Address Age

Use the following command to configure the MAC address aging timer:

Command	Description
mac-addr set mac-age <age>	Sets the length of time, in seconds, that a learned MAC address remains in the forwarding table without being used (how long a learned MAC address is allowed to remain idle before it is deleted from the table)
	Type the age in seconds from 10 to 1000000.

Displaying MAC Address Aging Timer Information

Use the following commands to display the MAC address aging timer information:

Commands	Description
mac-addr show mac-age	The mac-addr show mac-age command displays the current setting of the MAC address aging timer.
mac-addr show tbl <pre>{ vlan <vlan_id> mac <mac_addr> port <port#> all vlan <vlan_id> mac <mac_addr> }</pre>	<p>The mac-addr show tbl command displays the MAC address forwarding table. You can browse the table by VLAN ID, MAC address, port number, or all VLANs. Type one of the following:</p> <ul style="list-style-type: none"> vlan <vlan_id>—Type vlan and the VLAN ID. mac <mac_addr>—Type mac and the MAC address. port <port#>—Type port and the port number. all vlan <vlan_id> mac <mac_addr>—Type all vlan and the VLAN ID, and mac and MAC address.

This example shows the MAC address aging timer information.

```
>mac-addr show mac-age
Command: mac-addr show mac-age
Mac-aging time: 300
>
```

This example shows the MAC address monitoring table display for VLAN 1.

Command: mac-addr show tbl vlan 1

UID	MAC Address	Port	Status
1	00-00-77-83-D2-63	26	Dynamic
1	00-01-30-B8-D0-F0	26	Dynamic
1	00-02-A5-07-02-43	26	Dynamic
1	00-02-A5-D1-02-94	21	Dynamic
1	00-02-A5-D1-02-95	CPU	Self
1	00-08-02-3C-22-27	26	Dynamic
1	00-08-C7-4F-F5-01	26	Dynamic
1	00-08-C7-91-8F-9E	26	Dynamic
1	00-08-C7-CF-2C-6F	26	Dynamic
1	00-08-C7-E6-42-81	26	Dynamic
1	00-10-83-CF-B1-BD	26	Dynamic
1	00-50-8B-4A-B9-FD	26	Dynamic
1	00-50-8B-69-DB-4D	26	Dynamic
1	00-50-8B-DF-75-2D	26	Dynamic
1	00-50-8B-EB-08-DA	3	Dynamic
1	00-50-8B-EB-08-E1	21	Dynamic
1	00-50-8B-FE-CC-20	26	Dynamic
1	00-60-69-12-07-68	26	Dynamic
1	00-60-B0-87-AC-7A	26	Dynamic
1	00-60-B0-FB-CD-01	26	Dynamic

This example shows the MAC address monitoring table display for a MAC address.

>mac-addr show tbl mac 00-00-77-83-D2-63
Command: mac-addr show tbl mac 00-00-77-83-D2-63

UID	MAC Address	Port	Status
1	00-00-77-83-D2-63	26	Dynamic

>_

This example shows the MAC address monitoring table display for a port number.

```
Command: mac-addr show tbl port 26
```

UID	MAC Address	Port	Status
1	00-00-77-83-D2-63	26	Dynamic
1	00-01-30-B8-D0-F0	26	Dynamic
1	00-02-A5-07-02-43	26	Dynamic
1	00-08-02-3C-22-27	26	Dynamic
1	00-08-C7-4F-F5-01	26	Dynamic
1	00-08-C7-91-8F-9E	26	Dynamic
1	00-08-C7-CF-2C-6F	26	Dynamic
1	00-08-C7-E6-42-81	26	Dynamic
1	00-10-83-CF-B1-BD	26	Dynamic
1	00-50-8B-4A-B9-FD	26	Dynamic
1	00-50-8B-69-DB-4D	26	Dynamic
1	00-50-8B-DF-75-2D	26	Dynamic
1	00-50-8B-FE-CC-20	26	Dynamic
1	00-60-69-12-07-68	26	Dynamic
1	00-60-B0-87-AC-7A	26	Dynamic
1	00-60-B0-FB-CD-01	26	Dynamic
1	00-80-5F-0D-57-11	26	Dynamic
1	00-80-5F-A7-11-65	26	Dynamic
1	00-90-27-C6-5F-47	26	Dynamic
1	00-E0-2B-00-00-80	26	Dynamic

This example shows the MAC address monitoring table display for all VLANs.

```
>mac-addr show tbl all vlan 1 mac 08-00-69-08-9A-BC
Command: mac-addr show tbl all vlan 1 mac 08-00-69-08-9A-BC
```

UID	MAC Address	Port	Status
1	08-00-69-08-9A-BC	26	Dynamic

```
>_
```

Clearing MAC Address Monitoring Table

Use the following command to clear the MAC address monitoring table:

Command	Description
mac-addr clear port <portlist>	Clears the MAC address monitoring table for the specified port or ports

Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) snooping, when enabled and configured properly, manages multicast traffic through a switch module. IP multicast traffic is forwarded based on multicast group membership information registered by the switch module. The switch module can use IGMP snooping to configure ports dynamically, so that IP multicast traffic is forwarded only to those ports associated with IP multicast hosts, based on membership information.

IGMP snooping allows the switch module to recognize IGMP queries and reports sent between network stations or devices and an IGMP host that belongs to a specific multicast group. When enabled for IGMP snooping, the switch module can open or close a port to a specific device based on IGMP messages passing through the module. This feature further limits unnecessary broadcasts. The switch module can be configured to make queries using either IGMP version 1 or version 2.

When IGMP snooping is enabled globally on the switch module, you can enable or disable individual VLANs for IGMP snooping.

When IGMP snooping is enabled, any port receiving IGMP response packets will forward them to the CPU, and the CPU sets this port as a member of the corresponding multicast address.

The switch module supports three multicast group address filtering modes for making forwarding decisions regarding multicast packets.

- **Forward all group addresses**—All multicast packets destined for all group MAC addresses are forwarded according to the VLAN rules.
- **Forward all unregistered group addresses**—All multicast packets with group MAC address registration entries existing in the multicast table (both static multicast and group multicast created by IGMP snooping) are forwarded to member ports. If the group MAC address does not exist in the multicast table, packets are forwarded according to the VLAN rules.
- **Filter all unregistered group addresses**—All multicast packets with group MAC addresses are forwarded only if such forwarding is explicitly permitted by a group address entry in the multicast table. If the group MAC address exists in the multicast table, then the packets are forwarded using the port member list for that entry. If the group MAC address does not exist in the multicast table, the packets are dropped.

The following shows the factory default IGMP snooping settings:

Feature	Default Value
IGMP Snooping Globally	Disabled
Group Address Filter Mode	Forward all unregistered
IGMP Snooping—State	Enabled
IGMP Snooping—Querier State	Non-querier
IGMP Snooping—Robustness Variable	2
IGMP Snooping—Query Interval	125 seconds
IGMP Snooping—Max Response	10 seconds

Enabling IGMP Snooping

Use the following command to enable IGMP snooping:

Command	Description
igmp enable {feature vlan <vlan_id>}	<p>Enables the switch to read IGMP packets being forwarded through the switch in order to obtain forwarding information from them and learn which ports contain multicast members</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> feature—Type feature to enable IGMP snooping globally on the switch module. vlan <vlan_id>—Type vlan and the VLAN ID to enable IGMP snooping on a specific VLAN.

Disabling IGMP Snooping

Use the following command to disable IGMP snooping globally on the switch module or on a specified VLAN:

Command	Description
igmp disable {feature vlan <vlan_id>}	<p>Disables IGMP snooping globally on the switch module or on a specified VLAN</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none">• feature—Type feature to disable IGMP snooping globally on the switch module.• vlan <vlan_id>—Type vlan and the VLAN ID to disable IGMP snooping on a specific VLAN.

Setting IGMP Filter Mode for Processing Multicast Packets

Use the following command to set the IGMP filter mode for processing multicast packets:

Command	Description
igmp set filter {all unregistered filter}	<p>Sets IGMP filter mode for processing multicast packets and the parameters for VLAN-based IGMP snooping</p> <p>Type one of the following IGMP filter options in the command:</p> <ul style="list-style-type: none">• all—Forwards all packets.• unregistered—Forwards all packets with unregistered group addresses.• filter—Filters all packets with unregistered group addresses.

Adding IGMP Snooping Settings for a VLAN

Use the following command to add IGMP Snooping for a VLAN:

Command	Description
igmp add	Adds a VLAN to the IGMP snooping table and sets the IGMP snooping parameters
vlan <vlan_id>	Type the following in the command:
state {non v1 v2}	<ul style="list-style-type: none"> • vlan <vlan_id>—Type vlan and the VLAN ID.
robustness <robustness>	<ul style="list-style-type: none"> • state {non v1 v2}—Specifies the IGMP version (V1 or V2) that is used by the IGMP interface when making queries. Type state and one of the querier-state options: <ul style="list-style-type: none"> • non—non-querier • v1—version 1 querier • v2—version 2 querier
interval <query_interval>	<ul style="list-style-type: none"> • robustness <robustness>—Provides a tuning variable that allows for subnetworks that are expected to loose a large number of packets. Type robustness and a value from 2 to 225, with larger values being specified for subnetworks that are expected to loose larger numbers of packets. The default is 2.
response <response>	<ul style="list-style-type: none"> • interval <query_interval>—Specifies the length of time between sending IGMP queries. Type interval and a value from 1 to 65,500 seconds. The default is 125. • response <response>—Sets the maximum amount of time allowed before sending an IGMP response report. Type response and a value from 1 to 25 seconds. The default is 10 seconds.

Modifying IGMP Settings for a VLAN

Use the following command to modify the IGMP settings for a VLAN:

Command	Description
<pre>igmp modify vlan <vlan_id> { [state {non v1 v2}] [robustness <robustness>] [interval <query_interval>] [response <response>] }</pre>	<p>Modifies the parameters for a specified VLAN in the IGMP snooping table</p> <p>Type the VLAN ID and one or more of the following in the command:</p> <ul style="list-style-type: none"> • state {non v1 v2}—Specifies the IGMP version (V1 or V2) that is used by the IGMP interface when making queries. Type state and one of the querier-state options: <ul style="list-style-type: none"> • non—non-querier • v1—version 1 querier • v2—version 2 querier • robustness <robustness>—Provides a tuning variable that allows for subnetworks that are expected to lose a large number of packets. Type robustness and a value from 2 to 225, with larger values being specified for subnetworks that are expected to lose larger numbers of packets. The default is 2. • interval <query_interval>—Specifies the length of time between sending IGMP queries. Type interval and a value from 1 to 65500 seconds. The default is 125. • response <response>—Sets the maximum amount of time allowed before sending an IGMP response report. Type response and a value from 1 to 25 seconds. The default is 10.

Deleting IGMP Snooping Settings for a VLAN

Use the following command to delete an entry in the IGMP snooping table for a given VLAN:

Command	Description
igmp delete vlan <vlanlist>	Deletes an entry in the IGMP snooping table for a specified VLAN

Displaying IGMP Snooping Settings

Use the following command to display IGMP snooping settings:

Command	Description
igmp show { filter vlan {* <vlan_id>} status {* <vlan_id>} dynamic-reg }	<p>Displays IGMP snooping settings for a specific VLAN or VLANs</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> • filter—Type filter to display the IGMP filter mode. • vlan—Displays a list of all current settings for IGMP-enabled VLANs including IGMP State, Age Out, and Querier State. Age Out equals (Robustness Variable x Query Interval) + Maximum Response Time. Type vlan and one of the following: <ul style="list-style-type: none"> • * —Type an asterisk (*) to display all VLANs. • <vlan_id>—Type the VLAN ID to display the settings for a specified VLAN. • status—Displays the status for IGMP for all VLANs or for one VLAN. Type status and one of the following: <ul style="list-style-type: none"> • * —Type an asterisk (*) to display the status for all VLANs. • <vlan_id>—Type the VLAN ID to display the status for a specified VLAN. • dynamic-reg—Type dynamic-reg to display the Dynamic Group Registration Table. This table displays filtering information for VLANs configured into the bridge by local or network management, or learned dynamically. It specifies the set of ports to which frames received on a VLAN for this forwarding database, and containing a specific group destination address, are allowed to be forwarded.

This example shows the IGMP filter mode.

```
>igmp show filter
Command: igmp show filter

IGMP Filter mode :Forward All Unregistered

>_
```

This example shows the IGMP snooping settings for a VLAN.

```
>igmp show vlan 1
Command: igmp show vlan 1
```

UID	State	Age Out	Querier State
1	Enabled	260	Non-Querier

This example shows the IGMP snooping status.

```
>igmp show status 1
Command: igmp show status 1
```

UID	State	Querier State	Robustness Variable	Query Interval	Max Response
1	Enabled	Non-Querier	2	125	10

```
>_
```

This example shows the Dynamic Group Registration Table.

```
>igmp show dynamic-reg
Command: igmp show dynamic-reg
```

Dynamic Group Registration Table			
UID	Group Addr.	Type	Member Port-list

Configuring Class of Service, Default Port Priority, and Traffic Class

Class of Service (CoS) for packet prioritization allows you to set priority levels for forwarding packets based on the priority setting information in the packets.

The switch module supports four classes (0-3) of traffic (buffers or queues) per egress port. You can map eight priority levels (0-7) to the four queues. Traffic from a specific server port can be given priority over packets from other devices according to the range of priority levels. Seven (7) is the highest priority; zero (0) is the lowest priority. By default, queue 3 has the highest priority setting; queue 0 has the lowest priority setting.

You can set the following queue scheduling algorithms:

- **Strict Priority Based Scheduling (Strict):** If there are any packets residing in the high priority of the transaction, then they are taken up first for transmission.
- **Weighted Priority Based Scheduling (Round-robin):** This option provides continuous transmitting packet count at each queue. If the count is used up, the next priority queue is taken up for the transmission. The range of packet count is from 1 to 255 per queue.

You can also enable or disable a latency-based limit on a per queue basis. If any packet latency is greater than the maximum latency, the packet is dropped.

The following shows the CoS factory default settings:

Feature	Default Value
Scheduling Mechanism for CoS Queues	Strict
CoS—Max Packets	10
CoS—Max Latency	0
Default Port Priority	0
Class of Traffic	<ul style="list-style-type: none"> • Priority 0, 1: Class 0 • Priority 2, 3: Class 1 • Priority 4, 5: Class 2 • Priority 6, 7: Class 3

Setting Class of Service, Default Port Priority, and Traffic Class

Use the following command to set Class of Service (CoS), default port priority, and traffic class parameters:

Command	Description
<pre> cos set { sched {round-robin strict} queue class <class> max <max_packets> latency <latency> def-pri-tag tag <priority_tag> port <portlist> pri-map pri <priority_tag> class <class> } </pre>	<p>Defines the Class of Service (CoS) parameters for CoS queues (0-3)</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> sched {round-robin strict}—Sets 802.1p CoS queue forwarding option. Type sched and one of the following scheduling options: <ul style="list-style-type: none"> round-robin—Forwarding starts with the packets in the highest priority queue, moves to the queue with the next highest priority, and continues through to the queue with the lowest priority. At that point, forwarding returns to the queue with the highest priority. strict—When the highest priority queue is full, those packets are the first to be forwarded. queue—Defines the Class of Service parameters for Class of Traffic queues. Type queue and the following: <ul style="list-style-type: none"> class <class>—Sets the CoS queue. Type class and a value from 0 to 3. max <max_packets>—Sets the maximum packets to send for the class of a given port before moving to the next lower level of class. Type max and a value from 1 to 255. latency <latency>—Sets the maximum latency/time (in seconds) allowable for a packet to stay in the CoS queue. Type latency and a value from 0 to 255. def-pri-tag—Defines the default CoS priority-tag values (0-7) for the incoming non-priority tagged frames for a port or ports. Type def-pri-tag and the following: <ul style="list-style-type: none"> tag <priority_tag>—Type tag and a value from 0 to 7. port <portlist>—Type port and the port number or series of port numbers. pri-map—Set the mappings for priority tags to the CoS queue. Type pri-map and the following: <ul style="list-style-type: none"> pri <priority_tag>—Sets the priority tag value. Type pri and a value from 0 to 7. class <class>—Sets the Class of Traffic. Type class and a value from 0 to 3.

Displaying CoS Queue Information

Use the following command to display CoS queue information:

Command	Description
<pre>cos show { sched queue def-pri-tag <portlist> pri-map }</pre>	<p>Displays the current information for all CoS parameters and status</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> sched—Type sched to display the scheduling mechanism for 802.1p CoS queue. queue—Type queue to display the mapping of CoS priority to Class of Traffic queues on all switch ports. def-pri-tag <portlist>—Type def-pri-tag and the port number or numbers to display the current default CoS priority tag settings for the specified ports. pri-map—Type pri-map to display the mappings for priority tags to CoS queue.

This example shows the CoS queue scheduling mechanism.

```
>cos show sched
Command: cos show sched

Scheduling Mechanism for CoS Queues   : Strict
>_
```

This example shows the mapping of CoS priority to Class of Traffic queues.

```
>cos show queue
Command: cos show queue

Class      Max Packets      Max Latency
-----
0          10             0
1          10             0
2          10             0
3          10             0
>_
```


This example shows the current default CoS priority tag settings for a port.

```
>cos show pri-map
Command: cos show pri-map

Priority   Class
-----
0          0
1          0
2          1
3          1
4          2
5          2
6          3
7          3
>_
```

Configuring Port Trunking

Port trunking allows several ports to be grouped together to act as a single link. This provides a bandwidth that is a multiple of a single link bandwidth. Port trunking is most commonly used to link a bandwidth-intensive network device or devices, such as a server, to the backbone of a network.

The switch module allows the creation of up to six port trunk groups, each group consisting of up to eight links (ports). HP recommends that the port trunk ports be members of the same VLAN. Only similar type ports can be members of port trunks. A combination of Fast Ethernet (FE) and Gigabit (GE) ports cannot be members of the same port trunk.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the trunk group. This port is called the master port of the trunk group, and all configuration options, including the VLAN configuration, which can be applied to the master port, are applied to the entire port trunking group.

Load balancing is automatically applied to the ports in the trunked group, based on the setting of the trunk load-sharing algorithm, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

Spanning Tree Protocol treats a port trunking group as a single link on the switch module level. STP uses the port parameters of the master port in the calculation of port cost and in determining the state of the port trunking group. If two redundant port trunking groups are configured on the switch module, STP blocks one entire group, similar to STP blocking a link in case of two redundant links.

Considerations when Creating a Port Trunking Group

When creating a port trunking group, consider the following rules that determine how the port trunk reacts in network topology:

- The first port of the port trunk is implicitly configured to be the master logical port. This is the reference port used in configuration commands. It can be thought of as the logical port representing the entire group.
- When using a port trunk, always reference the master logical port of the group when configuring or viewing VLANs.
- VLANs configured to use other ports in the port trunk will have those ports deleted from the VLAN when the port trunk becomes enabled.
- The Spanning Tree algorithm views port trunk as a single Spanning Tree port. The Spanning Tree port is represented by the master logical port.
- If the VLAN settings of the master logical port are changed, the VLAN settings of all members of that port trunk are changed similarly.
- If the IGMP snooping configuration for any port trunk member is changed, the IGMP snooping settings for all port trunk members are changed.
- The port trunk takes precedence over any other setting. That is, the settings of trunked ports are the same as the master port settings.
- When any trunked port becomes a non-trunked port, all of the port configurations are reset to default settings.

Refer to Appendix G in the *HP ProLiant e-Class C-GbE Interconnect Switch User Guide* for additional information on port trunking.

The following shows the factory default port trunking settings:

Feature	Default Value
Port Trunking	Xconnect (Port 21–22)
Trunk Load-Sharing Algorithm	Source MAC Address

Creating a Port Trunk Group

Use the following command to create a new port trunk group:

Command	Description
trunk create name <group_name> id <group_id> status {enable disable} port <portlist>	<p>Creates a trunk definition with a group name, group ID, and the trunk status of enable or disable</p> <p>Type the following in the command:</p> <ul style="list-style-type: none">• name <group_name>—Type name and a group name from 1 to 15 characters in length.• id <group_id>—Type id and a group ID from 1 to 6.• status {enable disable}—Type status and either enable or disable a port trunking group. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device, or to have an absolute backup aggregation group that is not under automatic control.• port <portlist>—Type port and the port number or numbers to include as members of the trunk.

Adding a Port to an Existing Trunk

Use the following command to add a port or ports to trunk:

Command	Description
trunk add port id <group_id> port <portlist>	<p>Adds a port or ports to an existing trunk group</p> <p>Type the following in the command:</p> <ul style="list-style-type: none">• id <group_id>—Type id and the group ID number of the existing trunk.• port <portlist>—Type port and the port number or numbers to add to the trunk.

Deleting a Trunk Group or a Port from a Trunk Group

Use the following command to delete a trunk group or member ports from an existing trunk group:

Command	Description
<pre>trunk delete { id <group_id> entry id <group_id> port <portlist> }</pre>	<p>Deletes either a trunk group or a port from a trunk group</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> id <group_id>—Type id and the group ID number of the trunk to delete. entry—Type entry and the following: <ul style="list-style-type: none"> id <group_id>—Type id and the group ID number of the trunk. port <portlist>—Type port and the port number or numbers to delete from the trunk.

Enabling a Trunk Group

Use the following command to enable a trunk group:

Command	Description
trunk enable id <group_id>	Enables the specified trunk group

Disabling a Trunk Group

Use the following command to disable a trunk group:

Command	Description
trunk disable id <group_id>	Disables the specified trunk group

Clearing Trunk Utilization Counters

The switch module monitors the status of trunk utilization including the percentage of total available bandwidth being used by the group, the percentage of packets transmitted, and the percentage of packets being received per second. Use the following command to clear the trunk utilization counters:

Command	Description
trunk clear utilization	Clears the trunk utilization counters

Configuring the Trunk Load Sharing Algorithm Options

Use the following command to configure the load sharing algorithm options:

Command	Description
trunk set load-sharing { src-mac des-mac both }	<p>Sets the manner in which load sharing decisions will be determined</p> <p>Type one of the following algorithm options in the command:</p> <ul style="list-style-type: none">• src-mac—Type src-mac to set port selection based on the source MAC address.• des-mac—Type des-mac to set port selection based on the destination MAC address.• both—Type both to set port selection based on source and destination MAC address.

Displaying Trunk Load-Sharing Algorithm

Use the following command to display the load-sharing algorithm:

Command	Description
trunk show { id <group_id> utilization load-sharing }	<p>Displays the current information for trunk groups, trunk utilization status, and load sharing</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none">• id <group_id>—Displays the settings for a specific trunk group. Type id and the group ID number of the trunk.• utilization—Type utilization to display the trunk utilization status including the percentage of total available bandwidth being used by the group, the percentage of packets transmitted, and the percentage of packets being received per second.• load-sharing—Type load-sharing to display the load sharing status.

This example shows the settings for a trunk group.

```
>trunk show id 1
Command: trunk show id 1
```

ID	Group Name	State	PortList
1	XConnect	Enabled	21-22

```
>_
```

This example shows the trunk utilization status.

```
>trunk show utilization
Command: trunk show utilization
```

ID	Group Name	Member Ports	State	TX %utl	RX %utl	TX&RX %utl
1	XConnect	21-22	Enabled	0	1	1
2			Disabled	N/A	N/A	N/A
3			Disabled	N/A	N/A	N/A
4			Disabled	N/A	N/A	N/A
5			Disabled	N/A	N/A	N/A
6			Disabled	N/A	N/A	N/A

```
>_
```

This example shows the trunk load sharing algorithm.

```
>trunk show load-sharing
Command: trunk show load-sharing

Trunk Load Sharing Algorithm: Src Address
>
```

Configuring GVRP

GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q tagged ports.

GVRP updates dynamic VLAN registration entries and communicates the new VLAN registration information across the network. This feature allows stations to physically move to other switch module ports and keep their original VLAN settings, without having to reconfigure the VLAN settings on the switch module.

With GVRP, the switch module can

- Exchange VLAN configuration information with other GVRP switches.
- Prune unnecessary broadcast and unknown unicast traffic.
- Dynamically create and manage VLANs on switches connected through 802.1Q tagged ports.

The switch module provides options to enable or disable GVRP capability. If an 802.1Q tagged VLAN is enabled, but the GVRP is disabled, the only VLAN feature is static VLAN registration entries. HP recommends backing up static VLAN register entries to the configuration file.

If ingress filtering is enabled then the port will discard any frame received on that port whose VLAN classification does not include that port in its member set.

The following shows the GVRP factory default setting:

Feature	Default Value
Switch GVRP	Disabled

Enabling GVRP Globally or on a Per Port Basis

Use the following command to enable GARP VLAN Registration Protocol (GVRP) globally on the switch module. GVRP allows members to dynamically join VLANs:

Command	Description
gvrp enable { feature port <portlist> }	Enables GVRP globally on the switch module or on a specific port or ports Type one of the following in the command: <ul style="list-style-type: none">• feature—Type feature to enable GVRP globally on the switch.• port <portlist>—Type port and the port number or numbers to enable GVRP on the specified ports.

Disabling GVRP Globally or on a Per Port Basis

Use the following command to disable GVRP globally on the switch module:

Command	Description
gvrp disable { feature port <portlist> }	Disables GVRP globally on the switch module or on a specific port or ports Type one of the following in the command: <ul style="list-style-type: none">• feature—Type feature to disable GVRP globally on the switch.• port <portlist>—Type port and the port number or numbers to disable GVRP on the specified ports.

Displaying GVRP Settings

Use the following command to display the GVRP settings on the switch module:

Command	Description
gvrp show [port <portlist>]	Displays GVRP global configuration settings For port specific configuration settings, type port and the port number or numbers in the command.

This example shows GVRP settings for a specific port.

```
>gvrp show port 1
Command: gvrp show port 1

Global GVRP : Enabled
Port      state
-----
1         Enabled
>_
```

Configuring Telnet and Web Access Settings

The following shows the Telnet and Web access factory default settings:

Feature	Default Value
Telnet Status	Enabled
Web Status	Enabled

Enabling Telnet Access

Use the following command to enable Telnet access to the switch module:

Command	Description
telnet enable	Enables Telnet access to the switch module

Disabling Telnet Access

Use the following command to disable Telnet access to the switch module:

Command	Description
telnet disable	Disables Telnet access to the switch module



CAUTION: If you execute this command while in a Telnet session, you will lose the connection.

Displaying Telnet Access Settings

Use the following command to display Telnet access settings:

Command	Description
telnet show	Displays Telnet access settings

For example:

```
>telnet show
Command: telnet show

Telnet: Enabled
>_
```

Enabling Web Access

Use the following command to enable Web access:

Command	Description
web enable	Enables Web access to the switch module

Disabling Web Access

Use the following command to disable Web access:

Command	Description
web disable	Disables Web access to the switch module

Displaying Web Access Settings

Use the following command to display Web access settings.

Command	Description
web show	Displays Web access settings

For example:

```
>web show
Command: web show

Web: Enabled
>
```

Configuring Backpressure Flow Control

Backpressure can be enabled to initiate flow control on the switch module ports. When backpressure is enabled and there is incoming traffic congestion on a port, the receiving port sends a request to the transmitting port. The transmitting port acknowledges the request and stops sending packets for a random amount of time, before starting to send again.

The following shows the factory default setting for backpressure flow:

Feature	Default Value
Backpressure	Disabled

Enabling Backpressure Flow Control

Use the following command to enable backpressure flow control:

Command	Description
backpressure enable	Enables backpressure flow control on the switch module

Disabling Backpressure Flow Control

Use the following command to disable backpressure flow control:

Command	Description
backpressure disable	Disables backpressure flow control on the switch module

Displaying Backpressure Flow Control Settings

Use the following command to display backpressure flow control:

Command	Description
backpressure show	Displays backpressure flow control settings

For example:

```
>backpressure show
Command: backpressure show

Backpressure flow control: Disabled
>_
```

Configuring Switch Module Date and Time

The switch module can maintain the current date and time. This information displays on the management interfaces and is used to record the date and time of interconnect switch events in the history log.

When a new switch module is first booted up, the firmware clock starts at zero (0) and counts the seconds since bootup. In order for the clock to display the real date and time, you must either

- Manually set the date and time on the interconnect switch, or
- Enable Simple Network Time Protocol (SNTP) on the switch module, and then set the SNTP parameters.

SNTP allows the switch to synchronize its real time to the network time. When SNTP is enabled, the switch module sends a request to a primary SNTP server in each period of a specified polling interval asking for the Greenwich Mean Time (GMT). If the primary SNTP server is not available, the request is sent to a secondary SNTP server.

When SNTP is enabled, the following events cause the switch module to request the date and time through SNTP:

- The polling interval time expires.
- Changes are made to the configuration settings for Daylight Saving Time, time zone, SNTP Server 1 or Server 2, or polling interval .
- SNTP state is changed from disabled to enabled.

The following shows the SNTP factory default settings:

Feature	Default Value
SNTP	Disabled
SNTP Server 1	0.0.0.0
SNTP Server 2	0.0.0.0
SNTP Poll Interval	720 seconds
Time Zone	-06.00
Daylight Saving Time (DST)	Disabled
Offset in Minutes	60

Setting Date and Time Parameters Manually

IMPORTANT: If the system clock is set and power is lost to the interconnect switch, manual time settings are reset to factory defaults when the interconnect switch is powered on. If this occurs, manually reset the date and time. If SNTP is configured, losing power has no effect, so no manual resetting of time is required.

The factory default for SNTP is set to disabled. This allows you to manually set the date and time on the interconnect switch if desired. Use the time and date conventions in the following table when configuring the date, time, local time zone, and local daylight saving time parameters:

Table 2-2: Time and Date Conventions

Parameter	Format
Time	Type the time in hh:mm:ss format where <ul style="list-style-type: none"> • hh—Two-digit hour • mm—Two-digit minute • ss—Two-digit second For example, you would type 08:05:30 for five minutes and thirty seconds after 8 AM in the morning.
Date	Type a date in ddmthyyy format where <ul style="list-style-type: none"> • dd—Two-digit day of the month (01-31) • mth—First three characters of the name of the month: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec • yyyy—Four-digit year For example, you would type 05jun2002 for June 5, 2002.
Day of the Week	Type the first three letters of the weekday: sun, mon, tue, wed, thu, fri, sat.

IMPORTANT: SNTP must be set to disabled to manually set the time.

Use the following command to manually set the time, date, time zone, and daylight saving time parameters:

Command	Description
<pre> time set { [time <time>] [date <date>] [time-zone operator {+ -} hour <gmt_hour> min <minute>] [dst { disabled repeating s-which <start_which> s-day <start_day> s-mth <start_mth> s-time <start_time> e-which <end_which> e-day <end_day> e-mth <end_mth> e-time <end_time> offset <offset> annual s-date <start_date> s-mth <start_mth> s-time <start_time> e-date <end_date> e-mth <end_mth> e-time <end_time> offset <offset> }] } </pre>	<p>Manually sets the current time, date, time zone, and daylight saving time (DST) parameters</p> <p>Type the following in the command:</p> <ul style="list-style-type: none"> time <time>—Type time and the current time in hh:mm:ss format. date <date>—Type date and the current date in ddMTHyyy format. time-zone—Type time-zone and the following: <ul style="list-style-type: none"> operator {+ -}— Type (+) if the time is ahead of or (-) if the time is behind Greenwich Mean Time (GMT). hour <gmt_hour> min <minute>—Type hour and the hour and min and the number of minutes that the time zone is ahead or behind Greenwich Mean Time (GMT). dst—Type dst and disabled, repeating, or annual. Disabled disables the daylight saving time feature. Repeating allows you to set specific days of the week and month, for example the first Sunday in April through the fourth Sunday in October. Annual allows you to set specific dates for the year, for example April 3 through Oct. 27. <ul style="list-style-type: none"> s-which <start_which> and e-which <end_which>—Identify the starting and ending week of the month. Type s-which or e-which and 1, 2, 3, 4, or last. s-day <start_day> and e-day <end_day>—Identify the starting and ending day of the week. Type s-day or e-day the first three letters of the weekday: sun, mon, tue, wed, thu, fri, sat. s-mth <start_mth> and e-mth <end_mth>—Identifies the starting and ending month of the year. Type s-mth or e-mth a number from 1 to 12 (Example: October = 10). s-time <start_time> and e-time <end_time>—Identifies the starting and ending time. Type s-time or e-time and the time in hh:mm:ss format. offset <offset>—Identifies the number of minutes that the daylight saving time is offset from the current time. s-date <start_date> and e-date <end_date>—Identifies the starting and ending date. Type s-date or e-date in ddMTHyyy format.

Displaying Time Parameters

Use the following command to display the current time parameters:

Command	Description
time show	Displays the current switch time, up time or boot time (whichever is currently active), time zone settings, and daylight saving time settings

For example:

```
>time show
Command: time show

Current Time Source : System Clock
Boot Time          : 0 Days 00:00:00
Current Time       : 0 Days 21:12:24
Time zone          : GMT -06:00
Daylight Saving Time : Disabled
Offset in minutes  : 60
Repeating          : From : Apr 1st Sun 02:00
                   : To   : Oct last Sun 02:00
Annual            : From : 29 Apr 02:00
                   : To   : 12 Oct 02:00
>_
```

Enabling SNTP

In order for the switch module to synchronize its real time to the network time, you must first enable SNTP on the switch. After enabling SNTP, you must set the SNTP parameters.

Use the following command to enable SNTP on the switch module:

Command	Description
sntp enable	Enables SNTP

Setting SNTP Parameters

When SNTP is enabled on the switch module, it sends a request to a primary SNTP server in each period of a specified polling interval asking for Greenwich Mean Time (GMT). If the primary SNTP server is not available, the request is sent to a secondary SNTP server.

Use the following command to set the IP addresses for the primary and secondary SNTP server and specify the polling interval:

Command	Description
sntp set { [primary <ip_addr>] [secondary <ip_addr>] [poll-interval <poll_interval>] }	<p>Sets the IP address for the primary SNTP server and secondary SNTP server, and the polling interval for requesting the time from the server</p> <p>Type one or more of the following optional parameters in the command:</p> <ul style="list-style-type: none">• primary <ip_addr>—Type primary and the IP address for the primary SNTP server.• secondary <ip_addr>—Type secondary and the IP address for the secondary SNTP server.• poll-interval <poll_interval>—Sets the poll interval (in seconds) for requesting the time from the server. Type poll-interval and a number from 30 to 99999.

Displaying SNTP Parameters

Use the following command to display the SNTP parameters:

Command	Description
sntp show	Displays the following SNTP parameters: primary SNTP server IP address, secondary SNTP server IP address, and polling interval

For example:

```
>sntp show
Command: sntp show

Current Time Source : System Clock
SNTP : Disabled
SNTP Primary Server : 0.0.0.0
SNTP Secondary Server : 0.0.0.0
SNTP poll interval : 720 sec
>_
```

Disabling SNTP

Use the following command to disable SNTP on the switch module:

Command	Description
sntp disable	Disables SNTP SNTP must be set to disable in order to manually set the time and date.

Configuring Port Settings

The port commands allow you to configure the name, speed/duplex, flow control, and security settings for each port.

Speed/Duplex Settings

The speed-duplex parameter for each port can be set to 1000M/Full, 100M/Full, 100M/Half, 10M/Full, 10M/Half, or Auto. The Auto setting allows the port to automatically determine the fastest setting that the device to which the port is connected can handle.

IMPORTANT: In the forced 100M/Full, 100M/Half, 10M/Full, and 10M/Half modes, auto MDI-X is disabled and a cross-over cable must be used.

Port Security Settings

The port security feature controls the address learning capability and the traffic forwarding decisions for a port or ports. When enabled, you specify a number of source addresses to be learned (locked) at the port. Any incoming packets that do not have the learned source addresses are discarded.

The maximum number of learned addresses is ten. When the maximum number is reached, any incoming packet without one of the learned addresses is discarded, and no more new addresses can be learned at this port.

There are two modes for learned addresses.

- **Reset**—Tells the system to hold the learned addresses until the system is reset.
- **Timeout**—Tells the system to delete the addresses when the aging timer expires.

The following shows the factory default port settings:

Feature	Default Value
Port State	Enabled
Port Speed-Duplex	Auto
Flow Control	On
Port Security—Admin State	Disabled
Port Security—Max Address	1
Port Security—Mode	Delete On Reset

Setting Port Parameters

Use the following command to set the port parameters:

Command	Description
<pre>port set { label port <port#> name <name> params port <portlist> { [speed-duplex {auto 10-half 10-full 100-half 100-full 1000-full}] [flow-control {on off}] } security port <portlist> learn <max#> mode {timeout reset} }</pre>	<p>Configures the port names, port parameters, and port security parameters</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> • label—Sets the port name. Type label and the following: <ul style="list-style-type: none"> • port <port#>—Type port and the port number. • name <name>—Type name and a character string description for the port. 1-15 characters are allowed. • params—Sets the port parameters. Type params and the following: <ul style="list-style-type: none"> • port <portlist>—Type port and the port number or numbers, and one or both of the following: <ul style="list-style-type: none"> • speed-duplex {auto 10-half 10-full 100-half 100-full 1000-full}—Type speed-duplex and one of the speed-duplex options. <p>IMPORTANT: If the ports are Gigabit fiber, the only speed-duplex options are auto and 1000-full.</p> • flow-control {on off}—Type flow-control and either on or off. • security—Sets the port security parameters. Type security and the following: <ul style="list-style-type: none"> • port <portlist>—Type port and the port number or numbers. • learn <max#>—Type learn and the maximum number of addresses that can be learned at this port. A number from 0 to 10 is allowed. • mode {timeout reset}—Type mode and either timeout or reset.

Enabling Ports on a Per Port Basis

Use the following command to enable ports on a per port basis:

Command	Description
<pre>port enable { port <portlist> security <portlist> }</pre>	Enables ports on a per port basis. Disabled ports do not send or receive any traffic. The default is port enabled.

Disabling Ports or Port Security on a Per Port Basis

Use the following command to disable ports or port security on a per port basis:

Command	Description
<pre>port disable { port <portlist> security <portlist> }</pre>	<p>Disables ports or port security on a per port basis. Disabled ports do not send or receive any traffic. The default is port enabled.</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none">• port <portlist>—Disables the port or ports. Type port and the port number or numbers.• security <portlist>—Disables the security parameters for a port or ports. Type security and the port number or numbers.

Clearing Current Port Statistics

Use the following command to clear the current port statistics:

Command	Description
<pre>port clear { utilization port <portlist> error port <portlist> packet port <portlist> }</pre>	<p>Clears the utilization counters, error counters, or packet counters for a specified port or ports</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none">• utilization port <portlist>—Clears the utilization counters. Type utilization and the port number or numbers.• error port <portlist>—Clears the error counters. Type error and the port number or numbers.• packet port <portlist>—Clears the packet analysis counters. Type packet and the port number or numbers.

Displaying Current Port Settings and Port Names

Use the following command to display the current port settings and connection information for utilization, errors, packets, and security:

Command	Description
<pre>port show { utilization <portlist> error <portlist> packet <portlist> security <portlist> }</pre>	<p>Displays all the current port settings and current established connection information</p> <p>Type the one of following in the command:</p> <ul style="list-style-type: none"> utilization <portlist>—Type utilization and the port number or numbers to display the current number of packets transmitted and received per second and the percentage of the total available bandwidth being used. error <portlist>—Type error and the port number or numbers to display the current port error counters. packet <portlist>—Type packet and the port number or numbers to display the current packet analysis counters, including the size of packets received or transmitted and statistics on the number of unicast, multicast, and broadcast packets. security <portlist>—Type security and the port number or numbers to display the security parameters.

This example shows the current utilization for a group of ports.

```
>port show utilization 1-5
Command: port show utilization 1-5
```

Port	TX/sec	RX/sec	Util
1	0	0	0
2	0	0	0
3	0	1	1
4	0	0	0
5	1	0	1

```
>
```

This example shows the current errors for a group of ports.

```
>port show error 1-5
Command: port show error 1-5
```

Port number : 1			
	RX Frames		TX Frames
CRC Error	0	Excessive Deferral	0
Undersize	0		
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0

Port number : 2			
	RX Frames		TX Frames
CRC Error	0	Excessive Deferral	0
Undersize	0		
Oversize	0	Late Collision	0
Fragment	0	Excessive Collision	0
Jabber	0	Single Collision	0
Drop Pkts	0	Collision	0

This example shows the current packet count for a group of ports.

```
>port show packet 1-5
Command: port show packet 1-5
```

Port number : 1						
Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec	
64	101486	1	RX Bytes	0	0	
65-127	12661	0	RX Frames	0	0	
128-255	13367	0				
256-511	7482	0	TX Bytes	15711066	64	
512-1023	3803	0	TX Frames	138799	1	
1024-1518	0	0				
Unicast RX	0	0				
Multicast RX	0	0				
Broadcast RX	0	0				

■ CTRL+C [ESC] [F1] Quit [SPACE] [F2] Next Page [ENTER] Next Entry [F3] All _

This example shows the security parameters for a group of ports.

```
>port show security 1-5
Command: port show security 1-5
```

P#	Admin State	Max. Learning Addr.	Lock Address Mode
1	Disabled	1	Del On Reset
2	Disabled	1	Del On Reset
3	Disabled	1	Del On Reset
4	Disabled	1	Del On Reset
5	Disabled	1	Del On Reset

>_

Configuring Bandwidth

The switch module allows you to set a bandwidth limitation that restricts the ingress (receiving) and egress (transmitting) packet rate for each port. If the packet rate exceeds the allowed bandwidth rate, the excess packets will be dropped.

Bandwidth is configured in 1 to 127 units. Each unit is 117,481 bytes per second (around 0.94 Mb/s) for ports 1-26 and 939,850 bytes (about 7.52 Mb/s) for optional ports.

Adding and Configuring Restart Port Bandwidth Units

Use the following command to add and configure restart port bandwidth units:

Command	Description
<pre>bandwidth add port <portlist> { [ingress <bw_units>] [egress <bw_units>] }</pre>	<p>Adds a port to the restart ingress or egress bandwidth table and configures the bandwidth between 1 and 127 units of 117 Kbytes per second. Zero (0) means disable bandwidth control after restart.</p> <p>Type the port number or numbers in the command and one or both of the following options:</p> <ul style="list-style-type: none"> ingress <bw_units>—Type ingress and the number of ingress bandwidth units. A number between 1 and 127 is allowed. egress <bw_units>—Type egress and the number of egress bandwidth units. A number between 1 and 127 is allowed.

Deleting Ports from the Ingress and Egress Bandwidth Tables

Use the following command to delete ports from the ingress and egress bandwidth tables:

Command	Description
<pre>bandwidth delete port <portlist> { [ingress] [egress] }</pre>	<p>Deletes a port from the ingress or egress bandwidth table</p> <p>Type the port number or numbers in the command and one or both of the following bandwidth table options:</p> <ul style="list-style-type: none"> ingress—Deletes the port from the ingress (receiving) bandwidth table. egress—Deletes the port from the egress (transmitting) bandwidth table.

Modifying Ingress and Egress Bandwidth Parameters

Use the following command to modify ingress and egress bandwidth parameters:

Command	Description
bandwidth modify port <portlist> { [ingress <bw_units>] [egress <bw_units>] }	<p>Modifies a port to the restart ingress or egress bandwidth table and configures the bandwidth between 1 and 127 units of 117 Kbytes per second. Zero (0) means disable bandwidth control after restart.</p> <p>Type the port number or numbers and one or both of the following options:</p> <ul style="list-style-type: none"> • ingress <bw_units>—Type ingress and the number of ingress bandwidth units. A number between 1 and 127 is allowed. • egress <bw_units>—Type ingress and the number of egress bandwidth units. A number between 1 and 127 is allowed.

Displaying Current and Restart Port Bandwidth Settings

Use the following command to display the current and restart port bandwidth settings:

Command	Description
bandwidth show port <portlist> direction {ingress egress} type {current restart}	<p>Displays the current and restart port ingress or egress bandwidth settings</p> <p>Type the port number or numbers and the following.</p> <ul style="list-style-type: none"> • direction {ingress egress}—Type direction and either ingress or egress. • type {current restart}—Type type and either current or restart.

This example shows the restart ingress bandwidth settings for one port.

```
>bandwidth show port 1 direction ingress type restart
Command: bandwidth show port 1 direction ingress type restart
```

Port	Units	KBytes	Port Speed
1	50	5850	none

```
>
```

Configuring Spanning Tree Protocol

IEEE 802.1D Spanning Tree Protocol (STP) allows for the blocking of links between switches to avoid loops within the network. When multiple links between the switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once STP is configured and enabled, primary links are established and duplicated links are blocked and put into standby automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically, without operator intervention.

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

NOTE: Refer to Appendix D in the *HP ProLiant e-Class C-GbE Interconnect Switch User Guide* for more information on Spanning Tree Protocol.

The following shows the STP factory default setting:

Feature	Default Value
Switch STP	Enabled

Enabling STP

Spanning Tree Protocol (STP) can be enabled or disabled at the switch level. Only one spanning tree domain per switch module is supported. You can configure ports to participate in that spanning tree domain, by enabling or disabling the STP function on a per port basis. Ports can also be configured in STP bypass mode (fast forward mode) that allows the port to skip the initial STP states (listening and learning) before enabling it in the forwarding state.

IMPORTANT: The switch module supports mono-Spanning Tree Protocol. Multiple spanning tree domains are not supported. This means the Spanning Tree Algorithm makes calculations without considering the VLAN domains to which the ports belong. All ports that have STP enabled fall under one STP domain.

Use the following command to enable STP on the switch module, configure ports to participate in the spanning tree domain, or to enable bypass on a port.

Command	Description
stp enable { feature bypass <portlist> port <portlist> }	Enables STP on the switch module, enables a port or ports to participate in a single spanning tree domain, or enables bypass on a port or ports Type one of the following in the command: <ul style="list-style-type: none">• feature—Type feature to enable STP globally for the switch module.• bypass <portlist>—Type bypass and the port number or numbers to enable bypass on the specified ports.• port <portlist>—Type port and the port number or numbers to enable the port to participate in the spanning tree domain.

Disabling STP

Use the following command to disable STP on the switch module, disable ports from participating in the spanning tree domain, or to disable bypass on a port:

Command	Description
<pre> stp disable { feature bypass <portlist> port <portlist> }</pre>	<p>Disables STP on the switch module, disables a port or ports from participating in a single spanning tree domain, or disables bypass on a port or ports</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> • feature—Type feature to disable STP globally for the switch module. • bypass <portlist>—Type bypass and the port number or numbers to disable bypass on the specified ports. • port <portlist>—Type port and the port number or numbers to disable the port from participating in the spanning tree domain.

Setting Global and Per Port STP Parameters

The following STP settings can be configured globally on the switch module:

- **Bridging**—Sets the following bridging options:
 - **Forward delay**—Forward delay is the time any port on the switch module spends in the listening state while moving from the blocking state to the forwarding state. Forward delay values range from 4 to 30 seconds.
 - **Hello time**—Hello time is the interval between two transmissions of Bridge Protocol Data Units (BPDU) packets sent by the root bridge to tell all other switches that it is the root bridge. If you set a hello time for the switch module, and it is not the root bridge, the set hello time will be used if and when your switch module becomes the root bridge. The hello time cannot be longer than the maximum age, otherwise, a configuration error will occur. Hello time values range from 1 to 10 seconds.
 - **Max age**—Upon expiration of the maximum age, if a Bridge Protocol Data Unit (BPDU) has still not been received from the root bridge, the switch module will start sending its own BPDU to all other switches for permission to become the root bridge. If the switch module has the lowest bridge identifier, it will become the root bridge. Maximum values range from 6 to 40 seconds.
 - **Priority**—The priority number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a higher probability that this switch module will be elected as the root switch. Priority values range from 0 to 65,535. Zero (0) indicates the highest priority.

- **Port**—Sets the STP priority and port cost parameters for one port or a series of ports
 - **Priority**—This parameter sets the relative priority for the port. A lower number indicates a higher priority and a greater chance of the port being elected as the root port.
 - **Port cost**—Port cost is a value used by STP to evaluate paths. STP calculates port costs and selects the path with the minimum cost as the active path.

IMPORTANT: Observe the following formulas when setting the STP parameters on the root switch:

- $\text{Max Age} \leq 2 \times (\text{Forward Delay} - 1 \text{ second})$
- $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$

The following shows the factory default STP settings:

Feature	Default Value
Bridge Max Age	20 seconds
Bridge Hello Time	2 seconds
Bridge Forward Delay	15 seconds
Bridge Priority	32768
Port Priority	128
Port Cost	19 for ports 1-24 4 for ports 25-26

IMPORTANT: The factory default settings should be adequate for the majority of installations. HP recommends that you keep the default settings as set at the factory unless it is absolutely necessary to change them.

Use the following command to configure global and per port STP settings on the switch module:

Command	Description
<pre> stp set { bridging { [delay <forward_delay>] [time <hello_time>] [age <max_age>] [priority <prio>] } params port <portlist> { [priority <port_prio>] [cost <port_cost>] } } </pre>	<p>Sets bridging parameters or sets the per port priority or port cost parameters</p> <p>Type bridging and the bridging parameters or params and the parameter options in the command.</p> <ul style="list-style-type: none"> • bridging—Sets the bridging parameters forward delay, hello time, maximum age, and priority. Type bridging and one or more of the following: <ul style="list-style-type: none"> • delay <forward_delay>—Type delay and a value from 4 to 30 seconds. • time <hello_time>—Type time and a value from 1 to 10 seconds. • age <max_age>—Type age and a value from 6 to 40 seconds. • priority <prio>—Type priority and a value from 0 to 65,535. Zero (0) indicates the highest priority. • params port <portlist>—Sets the STP priority and port cost for one port or a series of ports. Type params port <portlist> and one or both of the following: <ul style="list-style-type: none"> • priority <port_prio>—Type priority and a priority number from 0 to 255. • cost <port_cost>—Type cost a port-cost number from 1 to 65535.

Displaying STP Bridging and Per Port Settings

Use the following command to display the STP bridging and per port settings:

Command	Description
stp show { [bridging] [port <portlist>] }	<p>Displays the STP bridging and per port settings for all ports</p> <p>Type one or both of the following in the command:</p> <ul style="list-style-type: none"> bridging—Type bridging to display bridging settings. port <portlist>—Type port and the port number or numbers to display STP settings for the specified ports.

This example the STP bridging settings.

```
>stp show bridging
Command: stp show bridging

STP Status      : Enabled
Max Age         : 20
Hello Time      : 2
Forward Delay   : 15
Priority        : 32768

Designated Root Bridge: 00-02-A5-D1-02-94
Root Priority    : 32768
Cost to Root    : 19
Root Port      : 21
Last Topology Change : 509457sec
Topology Changes Count: 4
>_
```

This example shows the STP settings for a series of ports.

```
>stp show port 1-12
Command: stp show port 1-12
```

Port	Conection	STP Status	Cost	Priority	ByPass	PortState
1	Link Down	Enabled	19	128	Yes	Disabled
2	Link Down	Enabled	19	128	Yes	Disabled
3	100M/Full/802.3x	Enabled	19	128	Yes	Forwarding
4	Link Down	Enabled	19	128	Yes	Disabled
5	100M/Full/802.3x	Enabled	19	128	Yes	Forwarding
6	Link Down	Enabled	19	128	Yes	Disabled
7	Link Down	Enabled	19	128	Yes	Disabled
8	Link Down	Enabled	19	128	Yes	Disabled
9	Link Down	Enabled	19	128	Yes	Disabled
10	Link Down	Enabled	19	128	Yes	Disabled
11	Link Down	Enabled	19	128	Yes	Disabled
12	Link Down	Enabled	19	128	Yes	Disabled

```
>
```

Configuring Static (Destination Address) Filtering Table

The switch module uses a filtering database to segment the network and control communications between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC address.

Each port on the switch module is a unique collision domain and the interconnect switch filters (discards) packets whose destination lies on the same port as it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever the switch module encounters a packet originating from or destined to a MAC address entered into the filter table, the interconnect switch will discard the packet.

Some filtering is performed automatically by the switch module, including:

- Dynamic filtering, which is automatic learning and aging of MAC addresses and their location on the network. Filtering keeps local traffic confined to its segment.
- Filtering performed by Spanning Tree Protocol to filter packets based on topology, making sure that signal loops do not occur.
- Filtering performed for VLAN integrity. Packets from a member of a VLAN destined for a device on another VLAN will be filtered.

Some filtering requires the manual entry of information into a filtering table. This includes MAC address filtering, which is the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry may be specified as source, destination, or both.

The following shows the static unicast and multicast filtering factory default settings:

Feature	Default Value
Static Unicast Filtering Table	None
Static Multicast Filtering Table	None

Adding Unicast Filter Actions

The switch module supports unicast filtering for static forwarding control. Packets are forwarded to a specific destination port (allow-to-go port) for a specific unicast destination address.

Use the following command to add unicast filter actions:

Command	Description
unicast add	Enables unicast filter actions
vlan <vlan_id>	Type the following in the command:
mac <mac_addr>	<ul style="list-style-type: none"> vlan <vlan_id>—Type vlan and the VLAN ID.
type {permanent delete-on-reset}	<ul style="list-style-type: none"> mac <mac_addr>—Type mac and the MAC address. type {permanent delete-on-reset}—Type type the one of the following filter types: <ul style="list-style-type: none"> permanent—The filter stays permanently until reconfigured. delete-on-reset—The filter is deleted when the port is reset.
port <port#>	<ul style="list-style-type: none"> port <port#>—Type port and the destination (allow-to-go) port number.

Modifying Unicast Filter Actions

Use the following command to modify unicast filter actions:

Command	Description
unicast modify	Modifies unicast filter actions
vlan <vlan_id>	Type the following in the command:
mac <mac_addr>	<ul style="list-style-type: none"> vlan <vlan_id>—Type vlan and the VLAN ID.
{ [type {permanent delete-on-reset}]	<ul style="list-style-type: none"> mac <mac_addr>—Type mac and the MAC address.
[port <port#>] }	Type one or both of the following options: <ul style="list-style-type: none"> type {permanent delete-on-reset}—Type type and one of the following filter types: <ul style="list-style-type: none"> permanent—The filter stays permanently until reconfigured. delete-on-reset—The filter is deleted when the port is reset. port <port#>—Type port and the port number for which you want to make modifications.

Deleting the Unicast Filter Actions

Use the following command to delete unicast filter actions:

Command	Description
unicast delete vlan <vlan_id> mac {<mac_addr> all }	<p>Deletes unicast filter actions for one or all MAC addresses on a VLAN</p> <p>Type the following in the command:</p> <ul style="list-style-type: none"> • vlan <vlan_id>—Type vlan and the VLAN ID. • mac {<mac_addr> all}—Type mac and one of the following: <ul style="list-style-type: none"> • <mac_addr>—Type the MAC address to delete. • all—Type all to delete all MAC addresses.

Displaying Unicast Filter Actions

Use the following command to display the current unicast filter actions for a specified VLAN:

Command	Description
unicast show [vlan <vlan_id>]	Displays unicast filtering settings for all VLANs or for the specific VLAN

This example shows the unicast filtering settings for a specific VLAN.

```
>unicast show vlan 1
Command: unicast show vlan 1

MAC Address      Vid    Port    Type
-----
>
```


Adding Multicast Filter Actions

The switch module supports forwarding control for group addresses. Packets are forwarded to specific ports of a group for a specific multicast destination address.

Use the following command to configure multicast filter actions:

Command	Description
multicast add	Enables multicast filter actions
vlan <vlan_id>	Type the following in the command:
mac <mac_addr>	<ul style="list-style-type: none">• vlan <vlan_id>—Type vlan and the VLAN ID.
type {permanent delete-on-reset}	<ul style="list-style-type: none">• mac <mac_addr>—Type mac and the MAC address.
port <portlist>	<ul style="list-style-type: none">• type {permanent delete-on-reset}—Type type and the filter type.<ul style="list-style-type: none">• permanent—The filter stays permanently until reconfigured.• delete-on-reset—The filter is deleted when the port is reset.• port <portlist>—Type port and the port number or numbers.

Modifying Multicast Filter Actions

Use the following command to configure multicast filter actions:

Command	Description
multicast modify	Modifies multicast filter actions
[vlan <vlan_id> mac <mac_addr>]	Type the following in the command:
[type {permanent delete-on-reset}	<ul style="list-style-type: none">• vlan <vlan_id>—Type vlan and the VLAN ID.
port <portlist>]	<ul style="list-style-type: none">• mac <mac_addr>—Type mac and the MAC address.
	Type one or both of the following options:
	<ul style="list-style-type: none">• type {permanent delete-on-reset}—Type type and the filter type.<ul style="list-style-type: none">• permanent—The filter stays permanently until reconfigured.• delete-on-reset—The filter is deleted when the port is reset.• port <portlist>—Type port and the port number or numbers.

Deleting Multicast Filter Actions

Use the following command to delete multicast filter actions:

Command	Description
multicast delete vlan <vlan_id> mac { <mac_addr> all }	Delete multicast filter actions for one or all MAC addresses on a VLAN Type the following in the command: <ul style="list-style-type: none"> • vlan <vlan_id>—Type vlan and the VLAN ID. • mac {<mac_addr> all}—Type mac and one of the following: <ul style="list-style-type: none"> • <mac_addr>—Type the MAC address of the VLAN on which you want to delete the multicast filter actions. • all—Type all to delete multicast filter actions on all MAC addresses.

Displaying Multicast Filter Settings for a VLAN

Use the following command to display the current multicast filter settings for a specified VLAN:

Command	Description
multicast show [vlan <vlan_id>]	Displays multicast filtering settings for all VLANs or a specific VLAN

This example shows the multicast filtering settings for a specific VLAN.

```
>multicast show vlan 1
Command: multicast show vlan 1
```

MAC Address	Uid	Type	PortList

>			

Configuring VLANs

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of physical LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that logical packets are forwarded only between ports within that VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily. VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

The switch module supports only port-based IEEE 802.1Q tag-capable VLANs.

VLAN membership for each port can be set as follows:

- **Egress Port**—This is a port on the interconnect switch that belongs to at least one VLAN. By default all ports are egress members of DEFAULT_VLAN.
 - **Untagged Member**—Ports that are untagged members of a VLAN participate in the VLAN, but no tag is associated to the packet when leaving that port. Untagged member ports can only be a member of one VLAN at a time.
 - **Tagged Member**—Ports with tagging enabled will insert the IEEE 802.1Q tag with the VID number into all packets that flow out of it. Tagged member ports can be members of multiple VLANs at a time, as packets are tagged with the VLAN ID from which they originated. Tagged member ports link IEEE 802.1Q trunks that work as inter-switch connections to forward packets belonging to multiple VLANs, to which those tagged member ports belong. If a packet has been tagged, the port does not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Forbidden Non-member**—These ports are not a member of the VLAN and are also forbidden from joining a VLAN dynamically when GVRP is enabled.

If ingress filtering is enabled for a port, the interconnect switch examines the VLAN information in the packet header (if present) and decides whether or not to forward the packet. The VID should match the PVID of that port, otherwise, that incoming packet is discarded.

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, it must do so through a router.

Default VLAN

The switch module reserves one VLAN, VID 1, also called DEFAULT_VLAN. The factory default setting assigns all ports on the switch module to the default VLAN. As new VLANs are configured, their respective member ports are removed from the default VLAN.

Characteristics of DEFAULT_VLAN include:

- DEFAULT_VLAN is an IEEE 802.1Q Static VLAN with VID equal to 1.
- DEFAULT_VLAN cannot be deleted.
- The VID cannot be changed. The VID that is equal to 1 is reserved for DEFAULT_VLAN.
- The VLAN name can be changed to any other valid VLAN name.
- You cannot delete a port from DEFAULT_VLAN, unless it is a member of another 802.1Q VLAN.
- You cannot forbid a port from DEFAULT_VLAN, unless it is a member of another 802.1Q VLAN.
- If a port is deleted from the only 802.1Q VLAN of which it is a member, then it will automatically become a member of DEFAULT_VLAN as an untagged, egress port.
- If a port is assigned to a user-created 802.1Q VLAN, and is **not** a tagged egress port member of DEFAULT_VLAN (in other words, it is an untagged egress port), then it will be deleted automatically from DEFAULT_VLAN.
- A tagged egress port of DEFAULT_VLAN will not be deleted from DEFAULT_VLAN, when it is assigned to another user-created 802.1Q VLAN.

The following shows the VLAN factory default settings:

Feature	Default Value
Static VLAN Entry	Default VLAN (VID = 1)
Port VLAN ID (PVID)	1
Port GVRP Setting	Off
Port Ingress Filtering	Off

Creating an 802.1Q Static VLAN

Use the following command to create a new 802.1Q static VLAN:

Command	Description
vlan create [name <vlan_name> id <vlan_id>] [forbid <portlist> egress [untagged <portlist> tagged <portlist>]]	<p>Creates a new 802.1Q static VLAN with VLAN ID and VLAN name settings</p> <p>The following are optional settings:</p> <ul style="list-style-type: none">• name <vlan_name>—Type name and a name to identify the VLAN that is 1 to 15 characters in length. Use an underscore (_) to connect words.• id <vlan_id>—Type vlan and a VLAN ID number. The number can be from 1 to 4094. Leading zeros are allowed, but not necessary. <p>The following are optional settings. If any of these are entered, each portlist must be mutually exclusive.</p> <ul style="list-style-type: none">• forbid <portlist>—Type forbid and the port number or numbers to define the ports that are forbidden from joining a VLAN dynamically.• egress—Type egress and one of the following:<ul style="list-style-type: none">• untagged <portlist>—Type untagged and the port number or numbers to define untagged ports. When the port transmits an untagged packet, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.• tagged <portlist>—Type tagged and the port number or numbers to define tagged ports. When the port transmits an untagged packet, the packet header is changed to include the 32-bit tag associated with the port VLAN identifier (PVID). When a tagged packet exits the port, the packet header is unchanged.

Adding a Port to an Existing VLAN

Use the following command to add a port or set of ports to an existing VLAN:

Command	Description
<pre> vlan add port id <vlan_id> { [forbid <portlist>] [egress { [untagged <portlist>] [tagged <portlist>] }] } </pre>	<p>Adds a port or a set of ports to an existing VLAN and allows the setting of the forbid and egress parameters</p> <p>Type the VLAN ID number and one or more of the following optional settings. Each portlist must be mutually exclusive. Ports not listed remain unchanged.</p> <ul style="list-style-type: none"> • forbid <portlist>—Type forbid and the port number or numbers to define ports that are forbidden from joining the VLAN dynamically. • egress—Type egress and one of the following: <ul style="list-style-type: none"> • untagged <portlist>—Type egress untagged and the port number or numbers to define untagged ports. When the port transmits an untagged packet, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet. • tagged <portlist>—Type egress tagged and the port number or numbers to define tagged ports. When the port transmits an untagged packet, the packet header is changed to include the 32-bit tag associated with the port VLAN identifier (PVID). When a tagged packet exits the port, the packet header is unchanged.

Deleting a VLAN or a Port from an Existing VLAN

Use the following command to delete a VLAN or delete a port from an existing 802.1Q static VLAN:

Command	Description
vlan delete { id <vlan_id> entry port <portlist> id <vlan_id> }	<p>Deletes a VLAN or a port or deletes a set of ports from an existing VLAN</p> <p>To delete a VLAN, type the following in the command:</p> <ul style="list-style-type: none">• id <vlan_id>—Type id and the ID of the VLAN to be deleted. <p>To delete a port or set of ports from an existing VLAN, type entry and the following in the command:</p> <ul style="list-style-type: none">• port <portlist>—Type port and the port number or numbers to be deleted.• id <vlan_id>—Type id and the ID of the VLAN for which the ports are members.

Modifying the Per Port VLAN Settings or VLAN Name

Use the following command to modify the per port settings or VLAN name:

Command	Description
<pre> vlan modify { port id <vlan_id> { [forbid <portlist>] [egress { [untagged <portlist>] [tagged <portlist>] }] } vlan id <vlan_id> name <vlan_name> } </pre>	<p>Changes the forbid and egress settings for a port or set of ports on an existing VLAN or changes the VLAN name</p> <p>To change the settings for a port or set of ports on an existing VLAN, type port id <vlan_id> and one or more of the following in the command:</p> <ul style="list-style-type: none"> • forbid <portlist>—Type forbid and the port number or numbers to define ports that are forbidden from joining the VLAN dynamically. • untagged <portlist>—Type untagged and the port number or numbers to define untagged ports. When the port transmits an untagged packet, the packet header remains unchanged. When a tagged packet exists the port, the tag is stripped and the packet is changed to an untagged packet. • tagged <portlist>—Type tagged and the port number or numbers to define tagged ports. When the port transmits an untagged packet, the packet header is changed to include the 32-bit tag associated with the port VLAN identifier (PVID). When a tagged packet exists the port, the packet header is unchanged. <p>IMPORTANT: Each portlist must be mutually exclusive.</p> <p>To change the name of an existing VLAN, type vlan and the following in the command:</p> <ul style="list-style-type: none"> • id <vlan_id>—Type id and the VLAN ID number. • name <vlan_name>—Type name and the new VLAN name.

Setting the PVID for a Port

Port VLAN ID (PVID) is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if Port 2 is assigned a PVID of 3, then all untagged packets received on Port 2 will be assigned to VLAN 3. This number is generally the same as the VID number assigned to the port.

Characteristics of a PVID include:

- By default, the PVID of all ports is the same as the VID of DEFAULT_VLAN, which is equal to 1.
- When a user creates an untagged 802.1Q VLAN and assigns a port, the PVID will be changed to the VID of that 802.1Q VLAN.
- For a tagged port, the PVID will be the same as the VID of the IEEE 802.1Q VLAN to which this port was first assigned.
- If the first IEEE 802.1Q VLAN to which the tagged port is assigned is deleted, the PVID will change to that of the second IEEE 802.1Q VLAN to which the port was assigned.
- The PVID of a port can only be set to a VID of a VLAN for which the port is already a member.

Use the following command to set the PVID for a port or set of ports:

Command	Description
vlan set pvid port <portlist> id <vlan_id>	Sets the PVID for the specified ports

Displaying VLAN Settings and Status

Use the following command to display the current VLAN settings and status:

Command	Description
<pre>vlan show { pvid <portlist> vlan <vlanlist> }</pre>	<p>Displays the current VLAN status, the current PVID settings, and the VLAN table information</p> <p>Type <code>vlan show</code> and one of the following:</p> <ul style="list-style-type: none"> pvid <portlist>—Type pvid and the port number of numbers. vlan <vlanlist>—Type vlan and the VLAN ID or IDs.

This example shows the current PVID settings for a series of ports.

```
>vlan show pvid 1-12
Command: vlan show pvid 1-12

  Port    PVID
  ----    -
  1        1
  2        1
  3        1
  4        1
  5        1
  6        1
  7        1
  8        1
  9        1
  10       1
  11       1
  12       1
>_
```

This example shows the current PVID settings for a specific VLAN.

```
>vlan show vlan 1
Command: vlan show vlan 1

VID  Name                1      8 9      16 17      24 25 26
----  -
1     DEFAULT_VLAN        UUUUUUUU UUUUUUUU UUUUUUUU U  U
      Status              Creation time
      -----
      Permanent           5 days 21:59:28
>
```

Enabling Ingress Filtering on a Per Port Basis

If ingress filtering is enabled for a port, the interconnect switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet. The VID should match the PVID of that port, otherwise, that incoming packet is discarded.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN.

- If the ingress port is not a member of the tagged VLAN, the packet is dropped.
- If the ingress port is a member of the 802.1Q VLAN, the interconnect switch then determines if the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port tags the packet with its own PVID as a VID (if the port is a tagging port). The interconnect switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port.

- If the destination port is not a member of the same VLAN, the packet is dropped.
- If the destination port is a member of the same VLAN, the packet is forwarded and the destination port transmits it on its attached network segment.

Ingress filtering is used to conserve bandwidth within the interconnect switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

The following shows the factory default setting for ingress filtering:

Feature	Default Value
Ingress-filtering	Off

Use the following command to enable ingress filtering on a per port basis:

Command	Description
ingress-filter enable port <portlist>	Enables ingress filtering on the specified port or ports

Disabling Ingress Filtering on a Per Port Basis

Use the following command to disable ingress filtering on a per port basis:

Command	Description
ingress-filter disable port <portlist>	Disables ingress filtering on a port or ports

Displaying Ingress Filtering Information

Use the following command to display the ingress filtering information on a per port basis:

Command	Description
ingress-filter show [port <portlist>]	Displays ingress filtering information for all ports To display ingress information for a specified port or ports, type port and the port number or numbers.

This example shows the ingress filtering information for a series of ports.

```
>ingress-filter show port 1-3
Command: ingress-filtering show port 1-3

  Port   Ingress
  ----   -
  1      Off
  2      Off
  3      Off
>
```

Configuring Port Mirroring

The switch module allows you to copy frames transmitted and received on a port (source) and redirect the copies to another port (target). You can attach a monitoring device to the mirrored (target) port, such as a sniffer or an RMON probe, to view details about the packets passing through the source port. This setting is useful for network monitoring and troubleshooting purposes.

The following configuration rules apply to any port mirroring configuration:

- A target mirror port cannot be configured as a trunk member.
- VLAN configuration settings for any ports configured for mirroring cannot be changed.
- The source and target ports should be members of the same VLAN.

The direction of traffic on the source port can be one of the following:

- Ingress traffic (received packets) on the source port
- Egress traffic (transmitted packets) on the source port
- Ingress and egress traffic on the source port

IMPORTANT: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 1000-Mb/s port onto a 100-Mb/s port, you can cause throughput problems. The port from which you are copying frames must support an equal or lower speed than the port to which you are sending the copies.

The following shows the port mirroring factory default settings:

Feature	Default Value
Port Mirroring—Source Port	1
Port Mirroring—Source Direction	Ingress and Egress
Port Mirroring—Target Port	11
Port Mirroring—Mirror Status	Disabled

Enabling Mirroring on a Port

Use the following command to enable mirroring on a port:

Command	Description
mirror enable src <src_port> target <target_port> type {tx rx both}	Enables mirroring on a port for network monitoring and troubleshooting purposes, and configuring source port, target port, and source traffic type Type the following in the command: <ul style="list-style-type: none">• src <src_port>—Type src and the source port number• target <target_port>—Type target and the target port number. The target port receives the copies from the source port. The target port is where you connect a monitoring or troubleshooting device such as a sniffer or an RMON probe.• type {tx rx both}—This defines the type of traffic to mirror. Type type and one of the following traffic directions:<ul style="list-style-type: none">• tx—Transmitting traffic of the port• rx—Receiving traffic of the port• both—Both transmitting and receiving traffic

Disabling Mirroring on a Port

Use the following command to disable mirroring on a port:

Command	Description
mirror disable	Disables the port mirroring function

Displaying Port Mirroring Status

Use the following command to display the port mirroring status:

Command	Description
mirror show	Displays mirroring information showing the source port, target port, traffic direction, and status of enabled or disabled

This example shows the port mirroring status.

```
>mirror show
Command: mirror show

Mirror Status      : Disabled
Target Port       : 11
Mirrored Port      : 1
Source Direction   : Ingress & Egress

>_
```

Configuring Thresholds for Broadcast, Multicast, DA-Unknown Storm Prevention or Monitoring

The switch module allows you to set a threshold (in packets per second) for three types of storms: broadcast, multicast, and one where the packet destination address (DA) is unknown. The higher the threshold, the more packets the switch module can accept per second. If the threshold is exceeded, any additional packets received are dropped. Entering a low value means packets have a greater chance to exceed the threshold and be dropped from the switch module.

The following shows the broadcast, multicast, and DA-unknown storm monitoring factory default settings:

Feature	Default Value
Broadcast Storm Monitoring	Disabled
Multicast Storm Monitoring	Disabled
Destination Address Unknown Storm Monitoring	Disabled
Storm Threshold	500 packets/second

Enabling Broadcast, Multicast, or Unknown Packet Storm Monitoring

Use the following command to enable broadcast, multicast, and DA-unknown storm monitoring:

Command	Description
monitor-storm enable { [broadcast] [multicast] [unknown] }	Enables monitoring of broadcast, multicast, or DA-unknown packet storm monitoring

Disabling Monitoring Broadcast, Multicast, DA-Unknown Storm Monitoring

Use the following command to disable monitoring broadcast, multicast, and DA-unknown storms:

Command	Description
monitor-storm disable { [broadcast] [multicast] [unknown] }	Disables monitoring of broadcast, multicast, or DA-unknown packet storms

Configuring Storm Threshold in Packets Per Second

Use the following command to configure the storm threshold in packets per second:

Command	Description
monitor-storm set threshold <threshold>	Sets threshold (in packets per second) to drop packets when broadcast, multicast, or DA-unknown packet rate exceeds this threshold Type a number between 0 and 262143 packets per second. The default is 500 packets per second.

Displaying Broadcast, Multicast, DA-Unknown Storm Current Settings

Use the following command to monitor the current settings for broadcast, multicast, and DA-unknown storm:

Command	Description
monitor-storm show	Displays the monitor storm settings, including the threshold information for broadcast, multicast, and DA-unknown packet storm

This example shows the current settings for broadcast, multicast, and unknown storm.

```
>monitor-storm show
Command: monitor-storm show

Broadcast           : Enabled
Multicast           : Enabled
Unknow DA           : Enabled
Threshold (Pkt/sec): 500
>
```

Configuring Priority MAC Address

The switch module can be set to force packets with specific destination MAC addresses and/or source MAC addresses to use specific Class of Service queues. This guarantees that those packets have a higher priority for forwarding. Refer to the “Configuring Class of Service, Default Port Priority, and Traffic Class” section for more information.

The following shows the port MAC address factory default settings:

Feature	Default Value
Priority MAC Address	None

Adding Priority Level for a MAC Address

Use the following command to add an entry into the priority MAC address table and set the priority level for a MAC address within a specified VLAN:

Command	Description
mac-pri add id <vlan_id> mac <mac_addr> priority <pri> look-at {src dest either}	Adds an entry into the priority MAC address table and sets the priority level for a MAC address within a specified VLAN Type the following in the command: <ul style="list-style-type: none">• id <vlan_id>—Type id and the VLAN ID.• mac <mac_addr>—Type mac and the MAC address.• priority <pri>—Type priority and a priority level between 0 and 7. Seven (7) is the highest priority level.• look-at {src dest either}—Sets the Look at MAC address filter. Type look-at and one of the following:<ul style="list-style-type: none">• src—Source MAC address• dest—Destination MAC address• either—Either source or destination MAC address

Deleting Priority Level for a MAC Address

Use the following command to delete a priority level for a MAC address within a specified VLAN:

Command	Description
mac-pri delete id <vlan_id> mac {<mac_addr> all}	Removes an entry from the priority MAC address table For a given VLAN, you can remove a single MAC address or remove all MAC addresses. Type the following in the command: <ul style="list-style-type: none">• id <vlan_id>—Type id and the VLAN ID.• mac {<mac_addr> all}—Type mac and MAC address or all to disable all MAC addresses.

Modifying Priority Level for a MAC Address

Use the following command to modify a priority level for a MAC address within a specified VLAN:

Command	Description
mac-pri modify id <vlan_id> mac <mac_addr> { [pri <pri>] [look-at { src dest either }] }	Modifies an entry in the priority MAC address table for a specified VLAN Type the following in the command: <ul style="list-style-type: none"> id <vlan_id>—Type id and the VLAN ID. mac <mac_addr>—Type mac and the MAC address. Type one or both of the following in the command: <ul style="list-style-type: none"> pri <pri>—Type pri and a priority level between 0 and 7. Seven (7) is the highest priority level. look-at {src dest either}—Sets the Look at MAC address filter. Type look-at and one of the following: <ul style="list-style-type: none"> src—Source MAC address dest—Destination MAC address either—Either source or destination MAC address

Displaying Current Priority Level for a MAC Address

Use the following command to display the current priority level for a MAC address:

Command	Description
mac-pri show [vlan <vlanlist>]	Displays current priority level for a MAC address all VLANs To display settings for a specified VLAN, type vlan and the list of VLANs in the command.

This example shows the current priority level settings for a MAC address.

```
>mac-pri show
Command: mac-pri show

UID      MAC Address      Priority  Look at
-----
>
```

Configuring the History Log

The history log displays a list of switch events, the sequence number of each event, the time of the event, and a description of the event.

Displaying the History Log

Use the following command to display the switch module history log:

Command	Description
log show	Displays the entries in the switch history log
[num <num>]	A defined number of entries can be displayed. Type the following in the command, where <num> is a set number of entries, <index> is a sequence number of a log entry, and an asterisk (*) means all: <ul style="list-style-type: none">• num <num>—Displays the last <num> entries• num *—Displays the entire history log• item <index>—Displays 20 entries starting with the defined index (sequence) number• item 0—Displays 20 entries starting at the beginning of the log• item <index> num <num>—Displays <num> entries starting with <index> sequence number• item 0 num <num>—Displays <num> entries starting at the beginning of the log• item <index> num *—Displays all entries starting at <index> sequence number
[item <index>]	

This example shows the history log.

Command: log show			
Seq.#	Time	Log Text	
122	5 days 22:09:40	Timeout through CLI	
121	5 days 22:06:57	Successful login through CLI	
120	5 days 22:06:57	Logout through CLI	
119	5 days 22:06:57	Successful login through cli.	
118	5 days 22:06:51	Successful login through telnet	
117	5 days 22:05:39	Timeout through CLI	
116	5 days 22:01:24	Successful login through CLI	
115	5 days 22:01:24	Logout through CLI	
114	5 days 22:01:24	Successful login through cli.	
113	5 days 22:01:14	Successful login through telnet	
112	5 days 21:39:35	Successful login through CLI	
111	5 days 21:39:35	Logout through CLI	
110	5 days 21:39:35	Successful login through cli.	
109	5 days 21:39:32	Fail login through CLI	
108	5 days 21:39:32	Login Failure	
107	5 days 21:39:28	Successful login through telnet	
106	5 days 16:01:02	Authentication Failure	
105	5 days 16:01:00	Authentication Failure	
104	5 days 16:00:58	Authentication Failure	
103	5 days 16:00:56	Authentication Failure	
CTRL+C ESC Quit SPACE Next Page ENTER Next Entry a All			

Clearing the History Log

Use the following command to clear the history log:

Command	Description
log clear	Clears the switch history log and resets the sequence number to 1

Configuring SNMP/RMON Manager

Simple Network Management Protocol (SNMP) is an Open Systems Interconnection (OSI) Layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as Insight Manager 7.

SNMP performs the following functions:

- Sends and receives SNMP packets through the IP protocol
- Collects information about the status and current configuration of network devices
- Modifies the configuration of network devices

The switch module has software, called an agent, that processes SNMP requests. The user program that makes the requests and collects the responses runs on the management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

The authentication protocol ensures that both the switch SNMP agent and the remote user SNMP application program discard packets from unauthorized users. SNMP (version 1) implements a form of security by requiring that each request include a “community string.” A community string is an arbitrary string of characters used as a “password” to control access to the switch module. If the switch module receives a request with a community name it does not recognize, it triggers an authentication trap.

Traps are messages that alert you of events that occur on the switch module. The events can be as serious as a reboot (someone accidentally reset the interconnect switch), or less serious like a configuration file update. The switch module generates traps and sends them to the network manager (trap recipient).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive traps sent from the switch module, and they may take certain actions to avoid future failure or breakdown of the network.

You can specify which network managers may receive traps from the interconnect switch by entering a list of the IP addresses of authorized network managers. Up to four trap-recipient IP addresses and four corresponding SNMP community strings can be entered.

In addition, the interconnect switch supports Remote Management (RMON) version 1, groups 1 (Statistics), 2 (History), 3 (Alarm), and 9 (Event).

The following shows the SNMP factory default settings:

Feature	Default Value
SNMP Community String	<ul style="list-style-type: none">• public• private
SNMP Community String Access Right	<ul style="list-style-type: none">• public = read-only• private = read/write
SNMP Trap Manager IP	None

Adding SNMP Management Interface Community Strings

SNMP allows up to four community names to be defined. The community names “public” and “private” are defined by default. You can change the names in addition to adding others. You must coordinate these names with the community name settings you use in your network management system.

Use the following command to configure the SNMP management interface community strings:

Command	Description
<pre>snmp add { string community <string> access {ro rw}] trap ip <ip_addr> community <string> }</pre>	<p>Configures the SNMP interface with up to four sets of community strings with access rights and access validity status and configures up to four (one at a time) SNMP trap manager IP addresses</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> • string —To define a community string, type string and the following: <ul style="list-style-type: none"> • community <string>—Type community and a string from 1 to 20 characters in length. This string is included on SNMP packets sent to and from the switch module. Any station not privy to this community does not receive the packet. • access {ro rw}—Type access and either ro (read only), meaning that the community member can only view switch settings, or rw (read-write) which allows the member to change settings on the switch module. • trap—To configure an SNMP trap IP address, type trap and the following: <ul style="list-style-type: none"> • ip <ip_addr>— Type ip and IP address of the trap recipient. • community <string>—Type community and a string from 1 to 20 characters in length.

Deleting SNMP Management Interface Community Strings

Use the following command to delete the SNMP management interface community strings:

Command	Description
<pre>snmp delete { community <string> ip <ip_addr> }</pre>	<p>Deletes an SNMP interface community string or an SNMP trap manager IP address</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> community <string> ip <ip_addr>

Displaying Current SNMP Management Interface Settings

Use the following command to display the current SNMP management interface settings:

Command	Description
<pre>snmp show [trap]</pre>	<p>Displays SNMP interface information including current settings of community strings with access rights</p> <p>Type trap in the command to display the current setting of the IP address of the trap manager, SNMP community string, and trap manager validity status.</p>

This example shows current SNMP management interface settings.

```
>snmp show
Command: snmp show
```

Community String	Rights	Access
public	Read-Only	Valid
private	Read/Write	Valid

```
>
```

Using System Utilities

The system utilities commands allow you to:

- Upgrade switch module firmware from a Trivial File Transfer Protocol (TFTP) server
- Upload the switch configuration settings to a file on a TFTP server
- Download the switch configuration settings from a file on a TFTP server
- Send the History Log to the TFTP server
- Perform a PING connectivity test

Setting TFTP

Trivial File Transfer Protocol (TFTP) services allow the switch firmware to be upgraded by transferring a new firmware file from a TFTP server to the switch module. A configuration file can also be loaded into the switch module from a TFTP server, switch module settings can be saved to the TFTP server, and a history log can be uploaded from the switch module to the TFTP server.

IMPORTANT: The TFTP server must be running TFTP server software to perform a file transfer. TFTP server software is included with the interconnect switch as part of the utilities package.

NOTE: A downloadable smart component, which further simplifies upgrading the GbE Interconnect Switch firmware, is available at the following website:

www.compaq.com/support/servers

The following shows the TFTP factory default settings:

Feature	Default Value
TFTP Server IP Address	0.0.0.0
TFTP Port Number	69
FW Filename	None
CFG Filename	None
Log Filename	None

Use the following command to set the parameters for TFTP file transfers.

Command	Description
tftp set { [ip <ip_addr>] [port <port_num>] [fw <path_filename>] [cfg <path_filename>] [log <path_filename>] }	<p>Sets the parameters for TFTP file transfers</p> <p>Type the following optional TFTP parameters in the command:</p> <ul style="list-style-type: none">• ip <ip_addr>—Type ip and the IP address for the TFTP server to use. The <ip_addr> default is 0.0.0.0.• port <port_num>—Type port and the port number to use for the TFTP server. The <port_num> default is 69.• fw <path_filename>—Type fw and the path and filename to use for a firmware file download command. The path name can be from 1 to 64 characters in length.• cfg <path_filename>—Type cfg and the path and filename to use for a configuration file upload or download command. The path name can from 1 to 64 characters in length.• log <path_filename>—Type log and the path and filename to use for a log file upload command. The path name can be from 1 to 64 characters in length.

Initiating a TFTP Download for Firmware or Configuration File

IMPORTANT: Configuration files used in the earlier version of the switch module (firmware version 1.0.0) are not supported by the present version (firmware version 2.0.0). Refer to the section “Displaying Switch Module Information” for information on how to display the current firmware version.

A configuration file can be downloaded from a TFTP server to the switch module. This file is then used by the switch module to configure itself. Beginning in firmware version 2.0.0, switch firmware configuration files are specified in XML format.

Downloaded XML configuration files do not need to specify every possible parameter. Only the configuration parameters specified will be modified; others will remain unchanged.

NOTE: For additional information, refer to Appendix H, XML Configuration, in the *HP ProLiant e-class C-GbE Interconnect Switch User Guide*.

Use the following command to initiate TFTP file transfers from the TFTP server.

Command	Description
tftp download type {fw cfg} [path <path_filename>] [ip <ip_addr>] [port <port_num>]	<p>Initiates TFTP file transfers from the TFTP server</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> • fw—Initiates TFTP download of a firmware file • cfg—Initiates TFTP download of a configuration file <p>The following optional parameters override their defaults only for the duration of this one command. These do not set the default.</p> <ul style="list-style-type: none"> • path <path_filename>—Type path and the path filename to use for a file download command. The path name can be from 1 to 64 characters in length. • ip <ip_addr>—Type ip and the IP address for the TFTP server to use. The <ip_addr> default is 0.0.0.0. • port <port_num>—Type port and the port number to use for the TFTP server. The <port_num> default is 69.

Initiating a TFTP Upload for Log File or Configuration File

The switch module configuration file and the history log can be uploaded from the switch to TFTP server storage. After completing the final configuration for the switch module, HP highly recommends that you save the configuration file to TFTP server storage. The switch module configuration file is saved in XML format.

IMPORTANT: For security reasons, user account information is not saved in the XML configuration file and must be managed by the switch module administrator. User account information can be manually added to the XML configuration file after it is uploaded, or it can be re-entered using the CLI, menu-driven interface, or Web interface.

Use the following command to initiate TFTP file transfers of the history log or configuration file to the TFTP server.

Command	Description
tftp upload type {log cfg} [path <path_filename>] [ip <ip_addr>] [port <port_num>]	<p>Initiates TFTP file transfers to the TFTP server</p> <p>Type one of the following in the command:</p> <ul style="list-style-type: none"> log—Initiates TFTP upload of a firmware file cfg—Initiates TFTP upload of a configuration file <p>The following optional parameters override their defaults only for the duration of this one command. These do not set the default.</p> <ul style="list-style-type: none"> path <path_filename>—Type path and the path filename to use for a file upload command. The path name can be from 1 to 64 characters in length. ip <ip_addr>—Type ip and the IP address for the TFTP server to use. The <ip_addr> default is 0.0.0.0. port <port_num>—Type port and the port number to use for the TFTP server. The <port_num> default is 69.

Displaying TFTP Parameters

Use the following command to display TFTP parameters.

Command	Description
tftp show	Displays the parameters used for TFTP file transfers

This example shows TFTP settings.

```
>tftp show
Command: tftp show

Server IP address: 0.0.0.0
TFTP server port : 69
FW filename      :
CFG filename     :
Log filename     :
>
```

Performing a Ping Test

Use the following command to run the ping utility:

Command	Description
ping <ip_addr> [<repeat>]	Pings the target IP address and repeats pinging infinitely or a specified number of times Type the target IP address in the command. To specify the number of times to ping, type a number from 0 to 244. Zero (0) means an infinite number of times. The default is 1. Press the ESC key to stop the ping.

Rebooting the Switch Module

Use the following command to reboot the switch:

Command	Description
reboot [{ cfg-save load-def save-ip-load-def }]	Reboots the switch module To save the configuration, type one of the following in the command: <ul style="list-style-type: none">• cfg-save—Type cfg-save to save the current configuration settings and reboot the switch module.• load-def—Type load-def to reboot the switch module to the factory default configuration settings.• save-ip-load-def—Type save-ip-load-def to reboot the switch module to the factory default configuration settings. This option allows the switch to retain its last IP address.

Logging Out

Use the following command to exit the current CLI session:

Command	Description
logout	Logs the user out of the current CLI session

Commands

Introduction

This appendix provides a summary of the commands supported by the interconnect switch command line interface (CLI). Refer to Chapter 2 for a detailed description of each command.

Using the Command Line Interface

Command	Description
menu	Toggles from the CLI to the menu-driven interface
def-interface set {menu cli}	Sets the default interface to either the menu-driven interface or the CLI
def-interface show	Displays the default interface
help [<command>]	Displays a complete list of available commands To display a help message for a specified command, type the command.
history	Displays the contents of the history buffer
history clear	Clears the history buffer
prompt <prompt_string>	Customizes the command prompt
clear	Clears the current CLI screen and displays a fresh page with a command prompt
paging {on off}	Configures the switch to display one page of data at a time

Saving Changes

Command	Description
cfg save	Saves current configuration settings to the switch NVRAM
cfg show	Displays current configuration settings

Managing User Accounts

Command	Description
user add user <username> access {r u+ u}	Adds a user account <ul style="list-style-type: none"> • r—root • u+—user + • u—user
user delete user <username>	Deletes the specified user's account
user show	Displays all user account information including each user's name and access level
user modify user <username> { [access {r u+ u}] [password] }	Modifies a user's account information

Configuring Remote Management IP Interface Settings

Command	Description
mgmt-if set { [mode {manual bootp dhcp}] [ipaddr <ip_addr>] [netmask <subnet_mask>] [def-gateway <ip_addr>] [mvid <vlan_id>] [secure-ip <iplist>] }	Sets the remote management parameters
mgmt-if show	Displays the remote management interface current IP and VLAN settings
mgmt-if delete secure-ip <iplist>	Deletes the secure IP addresses

Configuring Basic Switch Module Information

Command	Description
system set { [sysname <system_name>] [sysloc <system_location>] [contact <system_contact >] }	Configures system information
system show [advanced]	Displays basic switch information

Configuring Auto-Logout Timer

Command	Description
auto-logout set time-out {0 2 5 10 15}	Sets the auto-logout timer for idle timeout of the RS-232 console and Telnet management interface sessions
auto-logout show	Displays the current value set for the auto-logout timer for idle timeout of the RS-232 console and Telnet management interface sessions

Configuring MAC-Address Aging Timer

Command	Description
mac-addr set mac-age <age>	Sets the length of time, in seconds, that a learned MAC address remains in the forwarding table without being used (how long a learned MAC address is allowed to remain idle before it is deleted from the table)
mac-addr show mac-age	The mac-addr show mac-age command displays the current setting of the MAC-address aging timer.
mac-addr show tbl { vlan <vlan_id> mac <mac_addr> port <port#> all vlan <vlan_id> mac <mac_addr> }	The mac-addr show tbl command displays the MAC-address forwarding table.
mac-addr clear port <portlist>	Clears the MAC-address monitoring table for the specified port or ports

Configuring IGMP Snooping

Command	Description
igmp enable {feature vlan <vlan_id>}	Enables the switch to read IGMP packets being forwarded through the switch in order to obtain forwarding information from them and learn which ports contain multicast members
igmp disable {feature vlan <vlan_id>}	Disables IGMP snooping globally on the switch module or on a specified VLAN
igmp set filter {all unregistered filter}	Sets IGMP filter mode for processing multicast packets and the parameters for VLAN-based IGMP snooping
igmp add vlan <vlan_id> state {non v1 v2} robustness <robustness> interval <query_interval> response <response>	Adds a VLAN to the IGMP snooping table and sets the IGMP snooping parameters
igmp modify vlan <vlan_id> { [state {non v1 v2}] [robustness <robustness>] [interval <query_interval>] [response <response>] }	Modifies the parameters for a specified VLAN in the IGMP snooping table
igmp delete vlan <vlanlist>	Deletes an entry in the IGMP snooping table for a specified VLAN
igmp show { filter vlan {* <vlan_id> status {* <vlan_id> dynamic-reg }	Displays IGMP snooping settings for a specific VLAN or VLANs

Configuring Class of Service, Default Port Priority, and Traffic Class

Command	Description
cos set { sched {round-robin strict} queue class <class> max <max_packets> latency <latency> def-pri-tag tag <priority_tag> port <portlist> pri-map pri <priority_tag> class <class> }	Defines the Class of Service (CoS) parameters for CoS queues (0-3)
cos show { sched queue def-pri-tag <portlist> pri-map }	Displays the current information for all CoS parameters and status

Configuring Port Trunking

Command	Description
trunk create name <group_name> id <group_id> status {enable disable} port <portlist>	Creates a trunk definition with a group name, group ID, and the trunk status of enable or disable
trunk add port id <group_id> port <portlist>	Adds a port or ports to an existing trunk group
trunk delete { id <group_id> entry id <group_id> port <portlist> }	Deletes either a trunk group or a port from a trunk group
trunk enable id <group_id>	Enables the specified trunk group
trunk disable id <group_id>	Disables the specified trunk group
trunk clear utilization	Clears the trunk utilization counters
trunk set load-sharing { src-mac des-mac both }	Sets the manner in which load sharing decisions will be determined
trunk show { id <group_id> utilization load-sharing }	Displays the current information for trunk groups, trunk utilization status, and load sharing

Configuring GVRP

Command	Description
gvrp enable { feature port <portlist> }	Enables GVRP globally on the switch module or on a specific port or ports
gvrp disable { feature port <portlist> }	Disables GVRP globally on the switch module or on a specific port or ports
gvrp show [port <portlist>]	Displays GVRP global configuration settings

Configuring Telnet and Web Access Settings

Command	Description
telnet enable	Enables Telnet access to the switch module
telnet disable	Disables Telnet access to the switch module
telnet show	Displays Telnet access settings
web enable	Enables Web access to the switch module
web disable	Disables Web access to the switch module
web show	Displays Web access settings

Configuring Backpressure Flow Control

Command	Description
backpressure enable	Enables backpressure flow control on the switch module
backpressure disable	Disables backpressure flow control on the switch module
backpressure show	Displays backpressure flow control settings

Configuring Switch Module Date and Time

Command	Description
<pre> time set { [time <time>] [date <date>] [time-zone operator {+ -} hour <gmt_hour> min <minute>] [dst { disabled repeating s-which <start_which> s-day <start_day> s-mth <start_mth> s-time <start_time> e-which <end_which> e-day <end_day> e-mth <end_mth> e-time <end_time> offset <offset> annual s-date <start_date> s-mth <start_mth> s-time <start_time> e-date <end_date> e-mth <end_mth> e-time <end_time> offset <offset> }] } </pre>	<p>Manually sets the current time, date, time zone, and daylight saving time (DST) parameters. SNTP must be set to disabled to manually set the time.</p>
<pre> time show </pre>	<p>Displays the current switch time, up time or boot time (whichever is currently active), time zone settings, and daylight saving time settings</p>

Enabling Simple Network Time Protocol (SNTP)

sntp enable	Enables SNTP. SNTP allows the system to get the accurate time through the network.
sntp set { [primary <ip_addr>] [secondary <ip_addr>] [poll-interval <poll_interval>] }	Sets the IP address for the primary SNTP server and secondary SNTP server, and the polling interval for requesting the time from the server
sntp show	Displays the following SNTP parameters: primary SNTP server IP address, secondary SNTP server IP address, and polling interval
sntp disable	Disables SNTP SNTP must be set to disable in order to manually set the time and date.

Configuring Port Settings

Command	Description
<pre> port set { label port <port#> name <name> params port <portlist> { [speed-duplex {auto 10-half 10-full 100-half 100-full 1000-full}] [flow-control {on off}] } security port <portlist> learn <max#> mode {timeout reset} } } </pre>	Configures the port names, port parameters, and port security parameters
<pre> port enable { port <portlist> security <portlist> } </pre>	Enables ports or port security on a per port basis. Disabled ports do not send or receive any traffic. The default is port enabled.
<pre> port disable { port <portlist> security <portlist> } </pre>	Disables ports or port security on a per port basis. Disabled ports do not send or receive any traffic. The default is port enabled.
<pre> port clear { utilization port <portlist> error port <portlist> packet port <portlist> } </pre>	Clears the utilization counters, error counters, or packet counters for a specified port or ports

Configuring Port Settings *continued*

Command	Description
port show { utilization <portlist> error <portlist> packet <portlist> security <portlist> }	Displays all the current port settings and current established connection information

Configuring Bandwidth

Command	Description
bandwidth add port <portlist> { [ingress <bw_units>] [egress <bw_units>] }	Adds a port to the restart ingress or egress bandwidth table and configures the bandwidth between 1 and 127 units of 117 Kbytes per second
bandwidth delete port <portlist> { [ingress] [egress] }	Deletes a port from the ingress or egress bandwidth table
bandwidth modify port <portlist> { [ingress <bw_units>] [egress <bw_units>] }	Modifies a port to the restart ingress or egress bandwidth table and configures the bandwidth between 1 and 127 units of 117 Kbytes per second
bandwidth show port <portlist> direction {ingress egress} type {current restart}	Displays the current and restart port ingress or egress bandwidth settings

Configuring Spanning Tree Protocol

Command	Description
stp enable { feature bypass <portlist> port <portlist> }	Enables STP on the switch module, enables a port or ports from participating in a single spanning tree domain, or enables bypass on a port or ports
stp disable { feature bypass <portlist> port <portlist> }	Disables STP on the switch module, disables a port or ports from participating in a single spanning tree domain, or disables bypass on a port or ports
stp set { bridging { [delay <forward_delay>] [time <hello_time>] [age <max_age>] [priority <prio>] } params port <portlist> { [priority <port_prio>] [cost <port_cost>] } }	Sets bridging parameters or sets the per port priority or port cost parameters
stp show { [bridging] [port <portlist>] }	Displays the STP bridging and per port settings for all ports

Configuring Static (Destination Address) Filtering Table

Command	Description
unicast add vlan <vlan_id> mac <mac_addr> type {permanent delete-on-reset} port <port#>	Enables unicast filter actions
unicast modify vlan <vlan_id> mac <mac_addr> { [type {permanent delete-on-reset}] [port <port#>] }	Modifies unicast filter actions
unicast delete vlan <vlan_id> mac {<mac_addr> all}	Deletes unicast filter actions for one or all MAC addresses on a VLAN
unicast show [vlan <vlan_id>]	Displays unicast filtering settings for all VLANs or a specific VLAN
multicast add vlan <vlan_id> mac <mac_addr> type {permanent delete-on-reset} port <portlist>	Enables multicast filter actions
multicast modify [vlan <vlan_id> mac <mac_addr>] [type {permanent delete-on-reset} port <portlist>]	Modifies multicast filter actions
multicast delete vlan <vlan_id> mac { <mac_addr> all }	Deletes multicast filter actions for one or all MAC addresses on a VLAN
multicast show [vlan <vlan_id>]	Displays multicast filtering settings for all VLANs or for a specific VLAN

Configuring VLANs

Command	Description
vlan create [name <vlan_name> id <vlan_id>] [forbid <portlist> egress [untagged <portlist> tagged <portlist>]]	Creates a new 802.1Q static VLAN with VLAN ID and VLAN name settings
vlan add port id <vlan_id> { [forbid <portlist>] [egress { [untagged <portlist>] [tagged <portlist>] }] }	Adds a port or a set of ports to an existing VLAN and allows the setting of the forbid and egress parameters
vlan delete { id <vlan_id> entry port <portlist> id <vlan_id> }	Deletes a VLAN or a port or delete a set of ports from an existing VLAN
vlan modify { port id <vlan_id> { [forbid <portlist>] [egress { [untagged <portlist>] [tagged <portlist>] }] } vlan id <vlan_id> name <vlan_name> }	Changes the forbid and egress settings for a port or set of ports on an existing VLAN or changes the VLAN name

continued

Configuring VLANs *continued*

Command	Description
vlan set pvid port <portlist> id <vlan_id>	Sets the PVID for the specified ports
vlan show { pvid <portlist> vlan <vlanlist> }	Displays the current VLAN status, the current PVID settings, and the VLAN table information
ingress-filter enable port <portlist>	Enables ingress filtering on the specified port or ports
ingress-filter disable port <portlist>	Disables ingress filtering on a port or ports
ingress-filter show [port <portlist>]	Displays ingress filtering information for all ports

Configuring Port Mirroring

Command	Description
mirror enable src <src_port> target <target_port> type {tx rx both}	Enables mirroring on a port for network monitoring and troubleshooting purposes and configuring source port, target port, and source traffic type
mirror disable	Disables the port mirroring function
mirror show	Displays mirroring information showing the source port, target port, traffic direction, and status of enabled or disabled

Configuring Thresholds for Broadcast, Multicast, Unknown Storm Prevention or Monitoring

Command	Description
monitor-storm enable { [broadcast] [multicast] [unknown] }	Enables monitoring of broadcast, multicast, or unknown packet storm monitoring
monitor-storm disable { [broadcast] [multicast] [unknown] }	Disables monitoring of broadcast, multicast, or unknown packet storms
monitor-storm set threshold <threshold>	Sets threshold (in packets per second) to drop packets when broadcast, multicast, or unknown packet rate exceeds this threshold
monitor-storm show	Displays the monitor storm settings, including the threshold information for broadcast, multicast, and unknown packet storm

Configuring Priority MAC Address

Command	Description
mac-pri add id <vlan_id> mac <mac_addr> priority <pri> look-at {src dest either}	Adds an entry into the priority MAC address table and sets the priority level for a MAC address within a specified VLAN
mac-pri delete id <vlan_id> mac {<mac_addr> all}	Removes an entry from the priority MAC address table
mac-pri modify id <vlan_id> mac <mac_addr> { [pri <pri>] [look-at {src dest either}] }	Modifies an entry in the priority MAC address table for a specified VLAN
mac-pri show [vlan <vlanlist>]	Displays current priority level for a MAC address all VLANs

Configuring the History Log

Command	Description
log show [num <num>] [item <index>]	Displays the entries in the switch history log
log clear	Clears the switch history log and resets the sequence number to 1

Configuring SNMP Manager

Command	Description
snmp add { string community <string> access {ro rw} trap ip <ip_addr> community <string> }	Configures the SNMP interface with up to four sets of community strings with access rights and access validity status and configures up to four (one at a time) SNMP trap manager IP addresses
snmp delete { community <string> ip <ip_addr> }	Deletes an SNMP interface community string or an SNMP trap manager IP address
snmp show [trap]	Displays SNMP interface information including current settings of community strings with access rights

Using System Utilities

Command	Description
tftp set { [ip <ip_addr>] [port <port_num>] [fw <path_filename>] [cfg <path_filename>] [log <path_filename>] }	Sets the parameters for TFTP file transfers
tftp download type {fw cfg} [path <path_filename>] [ip <ip_addr>] [port <port_num>]	Initiates TFTP file transfers from the TFTP server
tftp upload type {log cfg} [path <path_filename>] [ip <ip_addr>] [port <port_num>]	Initiates TFTP file transfers to the TFTP server
tftp show	Displays the parameters used for TFTP file transfers
ping <ip_addr> [<repeat>]	Pings the target IP address and repeats pinging infinitely or a specified number of times

Rebooting the Switch Module

Command	Description
reboot [{cfg-save load-def save-ip-load-def}]	Reboots the switch module

Logging Out

Command	Description
logout	Logs the user out of the current CLI session

A

- accessing switch
 - procedure 1-2
- accounts, user 2-2
- advanced settings 2-9
- auto-logout 2-11, 2-13

B

- backpressure 2-12, 2-37
- bandwidth 2-49
- basic settings 2-9
- Bootstrap Protocol (BOOTP)
 - IP address assignment 2-6
- broadcast storm
 - configuring threshold 2-73

C

- Class of Service (CoS) 2-25
- class of traffic 2-25
- community names, SNMP 2-79
- component-level repairs ix
- configuration 1-1
- current egress bandwidth settings 2-49
- current ingress bandwidth settings 2-49

D

- date, configuring 2-38
- DA-unknown storm, configuring threshold 2-73
- default setting, resetting factory defaults 2-87
- Destination-Address Filtering Table 2-57
- DHCP (Dynamic Host Configuration Protocol)
 - IP address assignment 2-6
- Dynamic Group Registration Table 2-23

E

- egress bandwidth settings 2-49

F

- firmware upgrades 2-83
- flow control 2-37

G

- grounding ix
- grounding plug ix
- group address filter mode 2-12
- GVRP (GARP VLAN Registration Protocol)
 - settings 2-12, 2-33

H

- help resources x
- history, switch 2-78
- HP authorized reseller x

I

- IGMP (Internet Group Management Protocol)
 - snooping
 - advanced settings 2-11
 - overview 2-18
- IGMP Filter Mode 2-20
- ingress bandwidth settings 2-49
- ingress filtering 2-70
- Integrated Administrator (iA) connectors
 - accessing switch modules through 1-2
- IP addresses 2-5

L

- login procedures 1-2, 2-2
- logout procedures 2-87

M

- MAC address aging time 2-11, 2-14
- MAC addresses
 - configuring 2-75
- manual assignment of IP addresses 2-6
- mirroring of ports 2-71

multicast filtering 2-18, 2-57
multicast storm, configuring threshold 2-73

N

new users, setting up 2-2
NVRAM (non-volatile RAM) 2-1

P

packets, data
 monitoring 2-78
 prioritization service 2-25
ping test 2-87
port settings 2-43
port trunking 2-28
ports
 assigning VLANs to 2-68
 GVRP settings 2-12, 2-33
 mirroring of 2-71
priority MAC addresses 2-75
privileges, user 2-2
protocols, network
 BOOTP 2-6
 DHCP 2-6
 GVRP 2-12, 2-33
 SNMP 2-79
 SNTP 2-12, 2-38
PVID (port VLAN ID) 2-68

R

rebooting switch 2-87
remote management IP interface settings 2-5
restart egress bandwidth settings 2-49

S

saving changes 2-1
scheduling mechanism for CoS queues 2-12
size of packets, monitoring 2-78
SNMP (Simple Network Management Protocol) 2-79

SNTP (Simple Network Time Protocol) 2-12, 2-38
spanning tree protocol (STP) 2-51
static (Destination-Address Filtering) table 2-57
static VLAN entry 2-64

T

technician notes ix
telephone numbers x
Telnet
 settings 2-35
 status 2-12
TFTP (Trivial File Transfer Protocol) server 2-83
TFTP port number 2-12
time, configuring 2-38
traffic classes 2-25
trunk load sharing algorithm 2-12, 2-32
trunking feature 2-28

U

unicast filtering 2-57
upgrading firmware 2-83
users
 privilege levels 2-2
 setup procedures 2-2

V

ventilation clearances ix
VLANs (virtual local area networks) 2-62

W

warranty x
Web
 settings 2-35
 status 2-12