# HP Switch Software

## Management and Configuration Guide

2530-48G-PoE+
2530-24G-PoE+
2530-48G
2530-24G

Software version YA.15.10
November 2012

# HP Series 2530 Switches

**November 2012**
YA.15.10

# Management and Configuration Guide

**© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. All Rights Reserved.**

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

### Publication Number

5998-3456
November 2012

### Applicable Products

| | |
|---|---|
| HP Switch 2530-48G-PoE+ | (J9772A) |
| HP Switch 2530-24G-PoE+ | (J9773A) |
| HP Switch 2530-48G | (J9775A) |
| HP Switch 2530-24G | (J9776A) |

### Trademark Credits

Microsoft, Windows, and Microsoft Windows NT are US registered trademarks of Microsoft Corporation. Java™ is a US trademark of Sun Microsystems, Inc.

### Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

### Software End User License Agreement and Hardware Limited Warranty

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit www.hp.com/networking/support.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

*Hewlett-Packard Company*
*8000 Foothills Boulevard, m/s 5551*
*Roseville, California 95747-5551*
*http://www.hp.com/networking*

# Contents


## Product Documentation

**About Your Switch Manual Set . . . . . xv**

Electronic Publications . . . . . xv

## 1 Time Protocols

**Overview** . . . . . 1-1

TimeP Time Synchronization . . . . . 1-1

SNTP Time Synchronization . . . . . 1-1

**Selecting a Time Synchronization Protocol or Turning Off Time Protocol Operation** . . . . . 1-2

General Steps for Running a Time Protocol on the Switch: . . . . . 1-2

Disabling Time Synchronization . . . . . 1-3

**SNTP: Viewing, Selecting, and Configuring** . . . . . 1-3

Menu: Viewing and Configuring SNTP . . . . . 1-4

CLI: Viewing and Configuring SNTP . . . . . 1-7

Viewing the Current SNTP Configuration . . . . . 1-7

Configuring (Enabling or Disabling) the SNTP Mode . . . . . 1-9

**TimeP: Viewing, Selecting, and Configuring** . . . . . 1-14

Menu: Viewing and Configuring TimeP . . . . . 1-15

CLI: Viewing and Configuring TimeP . . . . . 1-16

Viewing the Current TimeP Configuration . . . . . 1-17

Configuring (Enabling or Disabling) the TimeP Mode . . . . . 1-18

**SNTP Unicast Time Polling with Multiple SNTP Servers** . . . . . 1-22

Displaying All SNTP Server Addresses Configured on the Switch . . 1-22

Adding and Deleting SNTP Server Addresses . . . . . 1-23

Menu: Operation with Multiple SNTP Server Addresses Configured . . . . . 1-23

**SNTP Messages in the Event Log** . . . . . 1-23

## 2 Port Status and Configuration


**Overview** . . . . . 2-1

**Viewing Port Status and Configuring Port Parameters** . . . . . 2-1

Menu: Port Status and Configuration . . . . . 2-2

Port Type . . . . . 2-2

Status of Ports . . . . . 2-3

Flow Control . . . . . 2-3

Broadcast Limit . . . . . 2-3

Modes . . . . . 2-4

Configuring Ports . . . . . 2-5

CLI: Viewing Port Status and Configuring Port Parameters . . . . . 2-6

Viewing Port Status and Configuration . . . . . 2-7

Customizing the Show Interfaces Command . . . . . 2-8

Error Messages . . . . . 2-10

Note on Using Pattern Matching with the "Show Interfaces Custom" Command . . . . . 2-11

Error Messages . . . . . 2-12

Note on Using Pattern Matching with the "Show Interfaces Custom" Command . . . . . 2-12

Viewing Port Utilization Statistics . . . . . 2-12

Viewing Transceiver Status . . . . . 2-13

Enabling or Disabling Ports and Configuring Port Mode . . . . . 2-14

Enabling or Disabling Flow Control . . . . . 2-15

Configuring a Broadcast Limit on the Switch . . . . . 2-17

Configuring Auto-MDIX . . . . . 2-18

Web: Viewing Port Status and Configuring Port Parameters . . . . . 2-21

**Jumbo Packets** . . . . . 2-21

Terminology . . . . . 2-22

Operating Rules . . . . . 2-22

Configuring Jumbo Packet Operation . . . . . 2-23

Overview . . . . . 2-23

Viewing the Current Jumbo Configuration . . . . . 2-23

Enabling or Disabling Jumbo Traffic on a VLAN . . . . . 2-25

Operating Notes for Jumbo Traffic-Handling . . . . . 2-25

Troubleshooting . . . . . 2-27

**Using Friendly (Optional) Port Names** . . . . . 2-28
Configuring and Operating Rules for Friendly Port Names . . . . . 2-28
Configuring Friendly Port Names . . . . . 2-29
Displaying Friendly Port Names with Other Port Data . . . . . 2-30
Configuring Transceivers That Haven't Been Inserted . . . . . 2-33
Transceivers . . . . . 2-33
**Uni-Directional Link Detection (UDLD)** . . . . . 2-34
Configuring UDLD . . . . . 2-35
Enabling UDLD . . . . . 2-36
Changing the Keepalive Interval . . . . . 2-37
Changing the Keepalive Retries . . . . . 2-37
Configuring UDLD for Tagged Ports . . . . . 2-37
Viewing UDLD Information . . . . . 2-38
Configuration Warnings and Event Log Messages . . . . . 2-39

## 3 Power Over Ethernet (PoE/PoE+) Operation

Configuration Options . . . . . 3-1
Related Publications . . . . . 3-2
Terminology . . . . . 3-2
**PoE Operation** . . . . . 3-3
Powered Device (PD) Support . . . . . 3-3
Power Priority Operation . . . . . 3-4
When Is Power Allocation Prioritized? . . . . . 3-4
How Is Power Allocation Prioritized? . . . . . 3-4
**Configuring PoE Operation** . . . . . 3-4
Disabling or Re-Enabling PoE Port Operation . . . . . 3-5
Enabling Support for Pre-Standard Devices . . . . . 3-5
Configuring the PoE Port Priority Level . . . . . 3-7
Controlling PoE Allocation . . . . . 3-8
Manually Configuring PoE Power Levels . . . . . 3-9
Changing the Threshold for Generating a Power Notice . . . . . 3-10
Cycling Power on a Port . . . . . 3-11
**PoE/PoE+ Allocation Using LLDP Information** . . . . . 3-12
LLDP with PoE . . . . . 3-12

LLDP with PoE+ . . . . . 3-13
Overview . . . . . 3-13
PoE Allocation . . . . . 3-13
Displaying PoE When Using LLDP Information . . . . . 3-14
Operating Note . . . . . 3-16
**Viewing PoE Configuration and Status** . . . . . 3-18
Displaying the Switch's Global PoE Power Status . . . . . 3-18
Displaying PoE Status on All Ports . . . . . 3-19
Displaying the PoE Status on Specific Ports . . . . . 3-21
**Planning and Implementing a PoE Configuration** . . . . . 3-22
Assigning PoE Ports to VLANs . . . . . 3-22
Applying Security Features to PoE Configurations . . . . . 3-22
**PoE Event Log Messages** . . . . . 3-23

## 4 Port Trunking

**Port Trunk Features and Operation** . . . . . 4-2
**Trunk Configuration Methods** . . . . . 4-3
**Menu: Viewing and Configuring a Static Trunk Group** . . . . . 4-7
**CLI: Viewing and Configuring Port Trunk Groups** . . . . . 4-9
Using the CLI To View Port Trunks . . . . . 4-9
Using the CLI To Configure a Static or Dynamic Trunk Group . . . . 4-12
**Web: Viewing Existing Port Trunk Groups** . . . . . 4-14
**Trunk Group Operation Using LACP** . . . . . 4-15
Default Port Operation . . . . . 4-17
LACP Notes and Restrictions . . . . . 4-18
**Trunk Group Operation Using the "Trunk" Option** . . . . . 4-21
**How the Switch Lists Trunk Data** . . . . . 4-22
**Outbound Traffic Distribution Across Trunked Links** . . . . . 4-22

## 5 Configuring for Network Management Applications

**Using SNMP Tools To Manage the Switch** . . . . . 5-1
Overview . . . . . 5-1

SNMP Management Features . . . . . 5-2
Configuring for SNMP version 1 and 2c Access to the Switch . . . . . 5-2
Configuring for SNMP Version 3 Access to the Switch . . . . . 5-3
SNMP Version 3 Commands . . . . . 5-4
Enabling SNMPv3 . . . . . 5-5
SNMPv3 Users . . . . . 5-5
Group Access Levels . . . . . 5-8
SNMPv3 Communities . . . . . 5-9
Menu: Viewing and Configuring non-SNMP version 3 Communities . . . . . 5-11
CLI: Viewing and Configuring SNMP Community Names . . . . . 5-12
SNMP Notifications . . . . . 5-14
Supported Notifications . . . . . 5-14
General Steps for Configuring SNMP Notifications . . . . . 5-15
SNMPv1 and SNMPv2c Traps . . . . . 5-16
Configuring an SNMP Trap Receiver . . . . . 5-16
Enabling SNMPv2c Informs . . . . . 5-18
Configuring SNMPv3 Notifications . . . . . 5-19
Managing Network Security Notifications . . . . . 5-23
Enabling Link-Change Traps . . . . . 5-24
Configuring the Source IP Address for SNMP Notifications . . . 5-25
Displaying SNMP Notification Configuration . . . . . 5-27
Advanced Management: RMON . . . . . 5-28
CLI-Configured sFlow with Multiple Instances . . . . . 5-28
Terminology . . . . . 5-28
Configuring sFlow . . . . . 5-29
Viewing sFlow Configuration and Status . . . . . 5-29
**LLDP (Link-Layer Discovery Protocol)** . . . . . 5-32
Terminology . . . . . 5-33
General LLDP Operation . . . . . 5-35
LLDP-MED . . . . . 5-35
Packet Boundaries in a Network Topology . . . . . 5-35
Configuration Options . . . . . 5-35
Options for Reading LLDP Information Collected by the Switch . . . 5-38
LLDP and LLDP-MED Standards Compatibility . . . . . 5-38

LLDP Operating Rules . . . . . 5-38
Configuring LLDP Operation . . . . . 5-40
Viewing the Current Configuration . . . . . 5-40
Configuring Global LLDP Packet Controls . . . . . 5-42
Configuring SNMP Notification Support . . . . . 5-45
Configuring Per-Port Transmit and Receive Modes . . . . . 5-46
Configuring Basic LLDP Per-Port Advertisement Content . . . . . 5-47
Configuring Support for Port Speed and Duplex Advertisements . . . . . 5-49
LLDP-MED (Media-Endpoint-Discovery) . . . . . 5-50
LLDP-MED Topology Change Notification . . . . . 5-52
LLDP-MED Fast Start Control . . . . . 5-54
Advertising Device Capability, Network Policy, PoE Status and Location Data . . . . . 5-54
Configuring Location Data for LLDP-MED Devices . . . . . 5-58
Displaying Advertisement Data . . . . . 5-63
Displaying Switch Information Available for Outbound Advertisements . . . . . 5-63
Displaying LLDP Statistics . . . . . 5-67
LLDP Operating Notes . . . . . 5-69
LLDP and CDP Data Management . . . . . 5-71
LLDP and CDP Neighbor Data . . . . . 5-71
CDP Operation and Commands . . . . . 5-72

## A File Transfers

**Downloading Switch Software** . . . . . A-1
General Software Download Rules . . . . . A-1
Using TFTP To Download Switch Software from a Server . . . . . A-2
Menu: TFTP Download from a Server to Primary Flash . . . . . A-2
CLI: TFTP Download from a Server to Flash . . . . . A-5
Using Secure Copy and SFTP . . . . . A-6
How It Works . . . . . A-8
The SCP/SFTP Process . . . . . A-8
Disable TFTP and Auto-TFTP for Enhanced Security . . . . . A-8
Command Options . . . . . A-10
Authentication . . . . . A-11

SCP/SFTP Operating Notes . . . . . A-11
Troubleshooting SSH, SFTP, and SCP Operations . . . . . A-13
Using Xmodem to Download Switch Software From a PC or UNIX Workstation . . . . . A-14
Menu: Xmodem Download to Primary Flash . . . . . A-15
CLI: Xmodem Download from a PC or UNIX Workstation to Primary or Secondary Flash . . . . . A-16
Switch-to-Switch Download . . . . . A-17
Menu: Switch-to-Switch Download to Primary Flash . . . . . A-17
CLI: Switch-To-Switch Downloads . . . . . A-18
Using IMC to Update Switch Software . . . . . A-19
**Copying Software Images** . . . . . A-19
TFTP: Copying a Software Image to a Remote Host . . . . . A-19
Xmodem: Copying a Software Image from the Switch to a Serially Connected PC or UNIX Workstation . . . . . A-20
**Transferring Switch Configurations** . . . . . A-20
TFTP: Copying a Configuration File to a Remote Host . . . . . A-21
TFTP: Copying a Configuration File from a Remote Host . . . . A-21
TFTP: Copying a Customized Command File to a Switch . . . . A-21
Xmodem: Copying a Configuration File to a Serially Connected PC or UNIX Workstation . . . . . A-22
Xmodem: Copying a Configuration File from a Serially Connected PC or UNIX Workstation . . . . . A-23
**Copying Diagnostic Data to a Remote Host, PC or UNIX Workstation** . . . . . A-24
Copying Command Output to a Destination Device . . . . . A-24
Copying Event Log Output to a Destination Device . . . . . A-25
Copying Crash Data Content to a Destination Device . . . . . A-25
Copying Crash Log Data Content to a Destination Device . . . . A-26

## B Monitoring and Analyzing Switch Operation

**Status and Counters Data** . . . . . B-1
Menu Access To Status and Counters . . . . . B-2
General System Information . . . . . B-3
Menu Access . . . . . B-3
CLI Access to System Information . . . . . B-3

Task Monitor—Collecting Processor Data . . . . . B-4
Switch Management Address Information . . . . . B-5
Menu Access . . . . . B-5
CLI Access . . . . . B-6
Port Status . . . . . B-6
Menu: Displaying Port Status . . . . . B-6
CLI Access . . . . . B-6
Web Access . . . . . B-7
Viewing Port and Trunk Group Statistics and Flow Control Status . B-7
Menu Access to Port and Trunk Statistics . . . . . B-8
CLI Access To Port and Trunk Group Statistics . . . . . B-9
Web Browser Access To View Port and Trunk Group Statistics . . . . . B-9
Viewing the Switch's MAC Address Tables . . . . . B-9
Menu Access to the MAC Address Views and Searches . . . . . B-10
CLI Access for MAC Address Views and Searches . . . . . B-12
Spanning Tree Protocol (MSTP) Information . . . . . B-13
CLI Access to MSTP Data . . . . . B-13
Internet Group Management Protocol (IGMP) Status . . . . . B-15
VLAN Information . . . . . B-15
Web Browser Interface Status Information . . . . . B-17
**Interface Monitoring Features** . . . . . B-17
Menu: Configuring Port and Static Trunk Monitoring . . . . . B-18
CLI: Configuring Port and Static Trunk Monitoring . . . . . B-19
Web: Configuring Port Monitoring . . . . . B-21
**Locating a Device** . . . . . B-22

## C Troubleshooting

**Troubleshooting Approaches** . . . . . C-1
**Browser or Telnet Access Problems** . . . . . C-2
**Unusual Network Activity** . . . . . C-3
General Problems . . . . . C-4
802.1Q Prioritization Problems . . . . . C-5
IGMP-Related Problems . . . . . C-5

LACP-Related Problems . . . . . C-6
Port-Based Access Control (802.1X)-Related Problems . . . . . C-6
QoS-Related Problems . . . . . C-9
Radius-Related Problems . . . . . C-9
Spanning-Tree Protocol (MSTP) and Fast-Uplink Problems . . . . . C-10
SSH-Related Problems . . . . . C-11
TACACS-Related Problems . . . . . C-13
TimeP, SNTP, or Gateway Problems . . . . . C-15
VLAN-Related Problems . . . . . C-15
Fan Failure . . . . . C-16
**Using the Event Log for Troubleshooting Switch Problems** . . . . C-17
Event Log Entries . . . . . C-17
Menu: Displaying and Navigating in the Event Log . . . . . C-22
CLI: Displaying the Event Log . . . . . C-23
CLI: Clearing Event Log Entries . . . . . C-24
CLI: Turning Event Numbering On or Off . . . . . C-24
Using Log Throttling to Reduce Duplicate Event Log and SNMP Messages . . . . . C-24
Log Throttle Periods . . . . . C-25
Example of Event Counter Operation . . . . . C-25
**Debug/Syslog Operation** . . . . . C-26
Debug/Syslog Messaging . . . . . C-26
Debug/Syslog Destination Devices . . . . . C-27
Debug/Syslog Configuration Commands . . . . . C-27
Configuring Debug/Syslog Operation . . . . . C-29
Displaying a Debug/Syslog Configuration . . . . . C-31
Debug Command . . . . . C-32
Debug Messages . . . . . C-33
Debug Destinations . . . . . C-35
Logging Command . . . . . C-36
Configuring a Syslog Server . . . . . C-37
Adding a Description for a Syslog Server . . . . . C-39
Adding a Priority Description . . . . . C-40
Adding a Description for a Syslog Server . . . . . C-41
Adding a Priority Description . . . . . C-41

Configuring the Severity Level for Event Log Messages Sent to a Syslog Server ..... C-42
Configuring the System Module Used to Select the Event Log Messages Sent to a Syslog Server ..... C-42
Operating Notes for Debug and Syslog ..... C-43
**Diagnostic Tools** ..... C-44
Port Auto-Negotiation ..... C-45
Ping and Link Tests ..... C-45
Web: Executing Ping or Link Tests ..... C-46
CLI: Ping Test ..... C-47
Link Tests ..... C-48
Traceroute Command ..... C-49
**Viewing Switch Configuration and Operation** ..... C-52
CLI: Viewing the Startup or Running Configuration File ..... C-52
Web: Viewing the Configuration File ..... C-53
CLI: Viewing a Summary of Switch Operational Data ..... C-53
Saving show tech Command Output to a Text File ..... C-54
CLI: Viewing More Information on Switch Operation ..... C-55
Pattern Matching When Using the Show Command ..... C-56
CLI: Useful Commands for Troubleshooting Sessions ..... C-59
**Restoring the Factory-Default Configuration** ..... C-60
CLI: Resetting to the Factory-Default Configuration ..... C-60
Clear/Reset: Resetting to the Factory-Default Configuration ..... C-60
**Restoring a Flash Image** ..... C-61
**DNS Resolver** ..... C-63
Terminology ..... C-63
Basic Operation ..... C-64
Configuring and Using DNS Resolution with DNS-Compatible Commands ..... C-66
Configuring a DNS Entry ..... C-66
Example Using DNS Names with Ping and Traceroute ..... C-68
Viewing the Current DNS Configuration ..... C-69
Operating Notes ..... C-70
Event Log Messages ..... C-71

## D MAC Address Management

**Determining MAC Addresses** . . . . . D-1

Menu: Viewing the Switch's MAC Addresses . . . . . D-2

CLI: Viewing the Port and VLAN MAC Addresses . . . . . D-3

**Viewing the MAC Addresses of Connected Devices** . . . . . D-4

## E Daylight Savings Time on HP Switches

## F Power-Saving Features

**Configuring Power-Saving** . . . . . F-1

Configuring the Savepower port-low-pwr Option . . . . . F-1

## Index

# Product Documentation

## About Your Switch Manual Set

**Note**

For the latest version of all HP switch documentation, including Release Notes covering recently added features, please visit the HP Networking web site at **www.hp.com/Networking/support**.

### Electronic Publications

The latest version of each of the publications listed below is available in PDF format on the ProCurve Web site, as described in the Note at the top of this page.

- *Installation and Getting Started Guide*—Explains how to prepare for and perform the physical installation and connect the switch to your network.
- *Basic Operation Guide*—Describes how to use the switch interfaces and introduces basic operations.
- *Management and Configuration Guide*—Describes how to configure, manage, and monitor basic switch operation.
- *Advanced Traffic Management Guide*—Explains how to configure traffic management features such as VLANs, MSTP, and QoS.
- *Access Security Guide*—Explains how to configure access security features and user authentication on the switch.
- *IPv6 Configuration Guide*—Describes the IPv6 protocol operations that are supported on the switch.
- *Event Log Message Reference Guide*—Provides a comprehensive description of event log messages.
- *Release Notes*—Describe new features, fixes, and enhancements that become available between revisions of the main product guide.

# Time Protocols

## Overview

This chapter describes:

- SNTP Time Protocol Operation
- Timep Time Protocol Operation

Using time synchronization ensures a uniform time among interoperating devices. This helps you to manage and troubleshoot switch operation by attaching meaningful time data to event and error messages.

The switch offers TimeP and SNTP (Simple Network Time Protocol) and a **timesync** command for changing the time protocol selection (or turning off time protocol operation).

**Notes**

- Although you can create and save configurations for both time protocols without conflicts, the switch allows only one active time protocol at any time.
- In the factory-default configuration, the time synchronization option is set to TimeP, with the TimeP mode itself set to **Disabled**.

### TimeP Time Synchronization

You can either manually assign the switch to use a TimeP server or use DHCP to assign the TimeP server. In either case, the switch can get its time synchronization updates from only one, designated Timep server. This option enhances security by specifying which time server to use.

### SNTP Time Synchronization

SNTP provides two operating modes:

- **Broadcast Mode:** The switch acquires time updates by accepting the time value from the first SNTP time broadcast detected. (In this case, the SNTP server must be configured to broadcast time updates to the network broadcast address. Refer to the documentation provided with your SNTP server application.) Once the switch detects a partic-

ular server, it ignores time broadcasts from other SNTP servers unless the configurable **Poll Interval** expires three consecutive times without an update received from the first-detected server.

**Note**

To use Broadcast mode, the switch and the SNTP server must be in the same subnet.

- **Unicast Mode:** The switch requests a time update from the configured SNTP server. (You can configure one server using the menu interface, or up to three servers using the CLI **sntp server** command.) This option provides increased security over the Broadcast mode by specifying which time server to use instead of using the first one detected through a broadcast.

# Selecting a Time Synchronization Protocol or Turning Off Time Protocol Operation

## General Steps for Running a Time Protocol on the Switch:

1. Select the time synchronization protocol: **SNTP** or **TimeP** (the default).
2. Enable the protocol. The choices are:
   - SNTP: **Broadcast** or **Unicast**
   - TimeP: **DHCP** or **Manual**
3. Configure the remaining parameters for the time protocol you selected.

   The switch retains the parameter settings for both time protocols even if you change from one protocol to the other. Thus, if you select a time protocol, the switch uses the parameters you last configured for the selected protocol.

Note that simply selecting a time synchronization protocol does not enable that protocol on the switch unless you also enable the protocol itself (step 2, above). For example, in the factory-default configuration, TimeP is the selected time synchronization method. However, because TimeP is disabled in the factory-default configuration, no time synchronization protocol is running.

### Disabling Time Synchronization

You can use either of the following methods to disable time synchronization without changing the Timep or SNTP configuration:

- In the System Information screen of the Menu interface, set the **Time Synch Method** parameter to **None**, then press **[Enter],** then **[S]** (for **Save**).
- In the Global config level of the CLI, execute **no timesync**.

# SNTP: Viewing, Selecting, and Configuring

| SNTP Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view the SNTP time synchronization configuration | n/a | page 1-4 | page 1-7 | — |
| select SNTP as the time synchronization method | timep | page 1-5 | page 1-9 ff. | — |
| disable time synchronization | timep | page 1-5 | page 1-13 | — |
| enable the SNTP mode (Broadcast, Unicast, or Disabled) | disabled | | | — |
| broadcast | n/a | page 1-5 | page 1-10 | — |
| unicast | n/a | page 1-5 | page 1-11 | — |
| none/disabled | n/a | page 1-5 | page 1-13 | — |
| configure an SNTP server address (for Unicast mode only) | none | page 1-5 | page 1-11 ff. | — |
| change the SNTP server version (for Unicast mode only) | 3 | page 1-6 | page 1-12 | — |
| change the SNTP poll interval | 720 seconds | page 1-6 | page 1-12 | — |
| change the server priority | n/a | — | page 1-11 | — |

**Table 1-1. SNTP Parameters**

| SNTP Parameter | Operation |
|---|---|
| **Time Sync Method** | Used to select either SNTP, TIMEP, or None as the time synchronization method. |
| **SNTP Mode** | |
| **Disabled** | The Default. SNTP does not operate, even if specified by the Menu interface **Time Sync Method** parameter or the CLI **timesync** command. |
| **Unicast** | Directs the switch to poll a specific server for SNTP time synchronization. Requires at least one server address. |
| **Broadcast** | Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval expires three times without the switch detecting a time update from the original server, it the switch accepts a broadcast time update from the next server it detects. |
| **Poll Interval (seconds)** | In Unicast Mode: Specifies how often the switch polls the designated SNTP server for a time update.<br>In Broadcast Mode: Specifies how often the switch polls the network broadcast address for a time update.<br>Value between 30-720 seconds. |
| **Server Address** | Used only when the **SNTP Mode** is set to **Unicast**. Specifies the IP address of the SNTP server that the switch accesses for time synchronization updates. You can configure up to three servers; one using the menu or CLI, and two more using the CLI. Refer to "SNTP Unicast Time Polling with Multiple SNTP Servers" on page 1-22. |
| **Server Version** | Default: 3; range: 1 - 7. Specifies the SNTP software version to use, and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3. |
| **Priority** | Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3. |

## Menu: Viewing and Configuring SNTP

To View, Enable, and Modify SNTP Time Protocol:

1. From the Main Menu, select:

   **2. Switch Configuration...**

      **1. System Information**

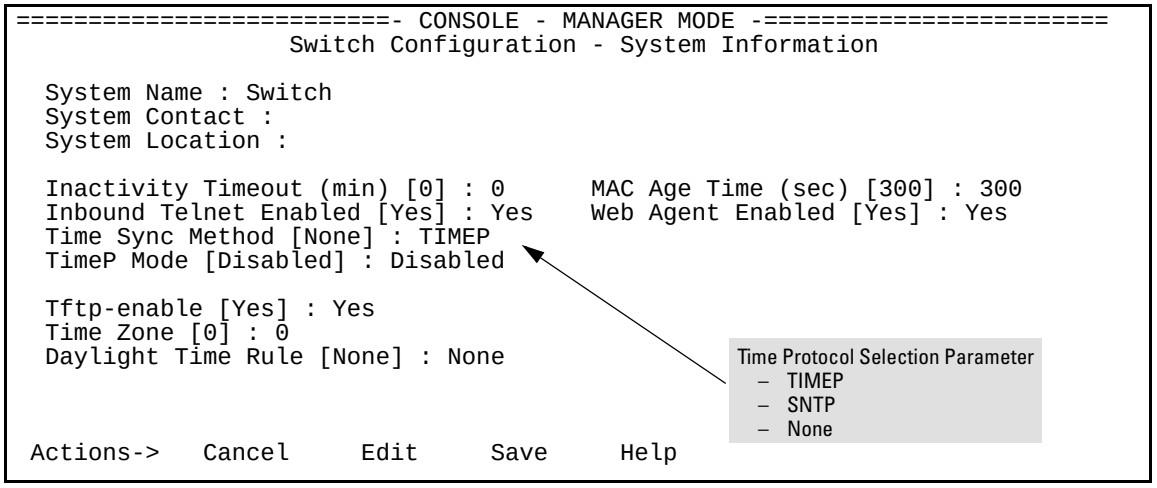



**Figure 1-1. The System Information Screen (Default Values)**

2. Press **[E]** (for **Edit**). The cursor moves to the **System Name** field.
3. Use ↓ to move the cursor to the **Time Sync Method** field.
4. Use the Space bar to select **SNTP**, then press ↓ once to display and move to the **SNTP Mode** field.
5. Do one of the following:
   - Use the Space bar to select the **Broadcast** mode, then press ↓ to move the cursor to the **Poll Interval** field, and go to step 6. (For Broadcast mode details, refer to "SNTP Operating Modes" on page 1-1.)

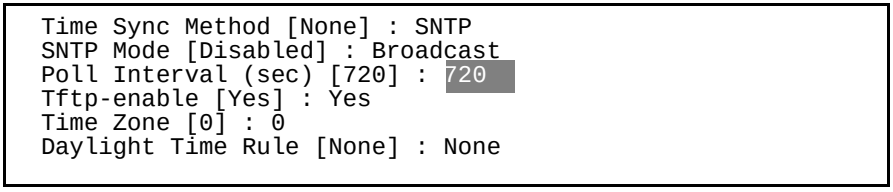



**Figure 1-2. Time Configuration Fields for SNTP with Broadcast Mode**

   - Use the Space bar to select the **Unicast** mode, then do the following:
     i. Press → to move the cursor to the **Server Address** field.
     ii. Enter the IP address of the SNTP server you want the switch to use for time synchronization.

**Note:** This step replaces any previously configured server IP address. If you will be using backup SNTP servers (requires use of the CLI), then refer to "SNTP Unicast Time Polling with Multiple SNTP Servers" on page 1-22.

iii. Press ↓ to move the cursor to the **Server Version** field. Enter the value that matches the SNTP server version running on the device you specified in the preceding step (step ii). If you are unsure which version to use, HP recommends leaving this value at the default setting of **3** and testing SNTP operation to determine whether any change is necessary.

**Note:** Using the menu to enter the IP address for an SNTP server when the switch already has one or more SNTP servers configured causes the switch to delete the primary SNTP server from the server list and to select a new primary SNTP server from the IP address(es) in the updated list. For more on this topic, refer to "SNTP Unicast Time Polling with Multiple SNTP Servers" on page 1-22.

iv. Press → to move the cursor to the **Poll Interval** field, then go to step 6.

```
Time Sync Method [None] : SNTP
SNTP Mode [Disabled] : Unicast        Server Address : 10.28.227.15
Poll Interval (sec) [720] : 720       Server Version [3] : 3
Tftp-enable [Yes] : Yes
Time Zone [0] : 0
Daylight Time Rule [None] : None
```

**Note:** The Menu interface lists only the highest priority SNTP server, even if others are configured. To view all SNTP servers configured on the switch, use the CLI **show management** command. Refer to "SNTP Unicast Time Polling with Multiple SNTP Servers" on page 1-22.

**Figure 1-3. SNTP Configuration Fields for SNTP Configured with Unicast Mode**

6. In the **Poll Interval** field, enter the time in seconds that you want for a Poll Interval. (For Poll Interval operation, see table 1-1, "SNTP Parameters", on page 1-4.)
7. Press **[Enter]** to return to the Actions line, then **[S]** (for **Save**) to enter the new time protocol configuration in both the startup-config and running-config files.

## CLI: Viewing and Configuring SNTP

CLI Commands Described in this Section

| SNTP Command | Page |
|---|---|
| show sntp | 1-7 |
| [no] timesync | 1-9, 1-10, 1-11, and 1-13 |
| sntp broadcast | 1-10 |
| sntp unicast | 1-11 |
| sntp server | 1-11 and ff. |
| Protocol Version | 1-9 and 1-11 |
| Priority | 1-9 and 1-11 |
| poll-interval | 1-12 |
| no sntp | 1-13 |

This section describes how to use the CLI to view, enable, and configure SNTP parameters.

## Viewing the Current SNTP Configuration

***Syntax:*** show sntp

> *This command lists both the time synchronization method (***TimeP***,* ***SNTP****, or* ***None****) and the SNTP configuration, even if SNTP is not the selected time protocol.*

For example, if you configured the switch with SNTP as the time synchronization method, then enabled SNTP in broadcast mode with the default poll interval, show sntp lists the following:

```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 719


  Priority SNTP Server Address                          Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                  7
  2        10.255.5.24                                   3
  3        fe80::123%vlan10                              3
```

**Figure 1-4. Example of SNTP Configuration When SNTP Is the Selected Time Synchronization Method**

In the factory-default configuration (where TimeP is the selected time synchronization method), **show sntp** still lists the SNTP configuration even though it is not currently in use. For example:

```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Timep
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 719


  Priority SNTP Server Address                          Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                  7
  2        10.255.5.24                                   3
  3        fe80::123%vlan10                              3
```

Even though, in this example, TimeP is the current time synchronous method, the switch maintains the SNTP configuration.

**Figure 1-5. Example of SNTP Configuration When SNTP Is Not the Selected Time Synchronization Method**

***Syntax:*** show management

*This command can help you to easily examine and compare the IP addressing on the switch. It lists the IP addresses for all time servers configured on the switch, plus the IP addresses and default gateway for all VLANs configured on the switch.*

```
HP Switch(config)# show management

 Status and Counters - Management Address Information

  Time Server Address : fe80::215:60ff:fe7a:adc0%vlan10

  Priority SNTP Server Address                          Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                  7
  2        10.255.5.24                                   3
  3        fe80::123%vlan10                              3


  Default Gateway     : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + ------------------
  DEFAULT_VLAN 001279-88a100       | Disabled
  VLAN10       001279-88a100       | 10.0.10.17
```

**Figure 1-6. Example of Display Showing IP Addressing for All Configured Time Servers and VLANs**

## Configuring (Enabling or Disabling) the SNTP Mode

Enabling the SNTP mode means to configure it for either broadcast or unicast mode. Remember that to run SNTP as the switch's time synchronization protocol, you must also select SNTP as the time synchronization method by using the CLI **timesync** command (or the Menu interface **Time Sync Method** parameter).

***Syntax:*** timesync sntp

*Selects SNTP as the time protocol.*

sntp < broadcast | unicast >

*Enables the SNTP mode (below and page 1-11).*

***Syntax:*** sntp server priority < 1 - 3 > < *ip-addr* | *ipv6-addr* > [1-7 ]

*Required only for unicast mode page 1-11). Provides SNTP server address, priority, and (optionally) the server version. The priority setting specifies the order in which the configured servers are polled for getting the time. The server version range is 1-7 and the default is 3.(page 1-11 ff.).*

***Note:*** *For more information about IPv6 addresses, refer to the IPv6 Configuration Guide for your switch.*

**Syntax:** sntp < 30 - 720 >

*Enabling the SNTP mode also enables the SNTP poll interval (default: 720 seconds; page 1-12).*

**Enabling SNTP in Broadcast Mode.** Because the switch provides an SNTP polling interval (default: 720 seconds), you need only these two commands for minimal SNTP broadcast configuration:

***Syntax:*** timesync sntp
*Selects SNTP as the time synchronization method.*

***Syntax:*** sntp broadcast
*Configures* **broadcast** *as the SNTP mode.*

For example, suppose:

- Time synchronization is in the factory-default configuration (TimeP is the currently selected time synchronization method).
- You want to:
  1. View the current time synchronization.
  2. Select SNTP as the time synchronization mode.
  3. Enable SNTP for Broadcast mode.
  4. View the SNTP configuration again to verify the configuration.

The commands and output would appear as follows:

```
HP Switch(config)# show sntp 1

 SNTP Configuration

  Time Sync Mode: Timep
  SNTP Mode : disabled
  Poll Interval (sec) [720] : 720

HP Switch(config)# timesync sntp 2

HP Switch(config)# sntp broadcast 3

5406_1(config)# show sntp 4

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 720
```

**show sntp** displays the SNTP configuration and also shows that TimeP is the currently active time synchronization mode.

**show sntp** again displays the SNTP configuration and shows that SNTP is now the currently active time synchronization mode and is configured for broadcast operation.

**Note:** The **Protocol Version** parameter will also appear in **show sntp** listings if the IP address of an SNTP server (used in Unicast mode) is configured in the switch. However, the protocol version is used only when SNTP is configured for Unicast operation. See "Enabling SNTP in Unicast Mode" on page 11.

**Figure 1-7. Example of Enabling SNTP Operation in Broadcast Mode**

**Enabling SNTP in Unicast Mode.** Like broadcast mode, configuring SNTP for unicast mode enables SNTP. However, for Unicast operation, you must also specify the IPv4 or IPv6 address and priority (1 - 3) of at least one SNTP server. The switch allows up to three unicast servers. You can use the Menu interface or the CLI to configure one IPv4 server address or to replace an existing IPv4 Unicast server address with another. To add an IPv6 server address or any second or third server address, you must use the CLI. For more on SNTP operation with multiple servers, refer to "SNTP Unicast Time Polling with Multiple SNTP Servers" on page 1-22.

***Syntax:*** timesync sntp

*Selects SNTP as the time synchronization method.*

***Syntax:*** sntp unicast

*Configures the SNTP mode for Unicast operation.*

***Syntax:*** sntp server priority < 1 - 3 > < *ip-addr* | *ipv6-addr* > [ 1 - 7 ]

*Specifies the SNTP server address, server priority, and (optionally) the server version. The priority setting (1-3) specifies the order in which the configured servers are polled for getting the time.The server version range is 1-7 and the default is 3.*

***Syntax:*** no sntp server < *ip-addr* | *ipv6-addr* >

*Deletes the specified SNTP server.*

**Note**

Deleting an SNTP server when only one is configured disables SNTP unicast operation.

For example, to select SNTP and configure it with unicast mode and an SNTP server at 10.28.227.141 with a server priority of 2, default server version (3), and default poll interval (720 seconds):

```
HP Switch(config)# timesync sntp
```

*Selects SNTP.*

```
HP Switch(config)# sntp unicast
```

*Activates SNTP in Unicast mode.*

```
HP Switch(config)# sntp server priority 2 10.28.227.141
```

*Specifies the SNTP server with a priority of "2" and accepts the current SNTP server version (default: 3).*

```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 720


  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.28.227.141                                    3
  3        fe80::123%vlan10                                 3
```

In this example, the **Poll Interval** and the **Protocol Version** appear at their default settings.

Both IPv4 and IPv6 addresses are displayed.

**Note:** Protocol Version appears only when there is an IP address configured for an SNTP server.

**Figure 1-8. Example of Configuring SNTP for Unicast Operation**

If the SNTP server you specify uses SNTP version 4 or later, use the **sntp server** command to specify the correct version number. For example, suppose you learned that SNTP version 4 was in use on a server you specified above (IP address 10.28.227.141) with version 3. You would use the following commands to delete the server IP address and then re-enter it with the correct version number for that server:

```
HP Switch(config)# no sntp server priority 2 10.28.227.141
HP Switch(config)# sntp server priority 2 10.28.227.141 4
5406_1(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 720


  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.28.227.141                                    4
  3        fe80::123%vlan10                                 3
```

Deletes unicast SNTP server entry.

Re-enters the unicast server with a non-default protocol version.

**show sntp** displays the changed server protocol version.

**Figure 1-9. Example of Specifying the SNTP Protocol Version Number**

### Changing the SNTP Poll Interval.

***Syntax:*** sntp < 30..720 >

*Specifies how long the switch waits between time polling intervals. The default is 720 seconds and the range is 30 to 720 seconds. (This parameter is separate from the poll interval parameter used for Timep operation.)*

For example, to change the poll interval to 300 seconds:

```
HP Switch(config)# sntp poll-interval 300
```

**Disabling Time Synchronization Without Changing the SNTP Configuration.** The recommended method for disabling time synchronization is to use the **timesync** command.

***Syntax:*** no timesync

*Halts time synchronization without changing your SNTP configuration.*

For example, suppose SNTP is running as the switch's time synchronization protocol, with **Broadcast** as the SNTP mode and the factory-default polling interval. You would halt time synchronization with this command:

```
HP Switch(config)# no timesync
```

If you then viewed the SNTP configuration, you would see the following:

```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Disabled
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 720
```

**Figure 1-10. Example of SNTP with Time Sychronization Disabled**

**Disabling the SNTP Mode.** If you want to prevent SNTP from being used even if selected by **timesync** (or the Menu interface's **Time Sync Method** parameter), configure the SNTP mode as disabled.

***Syntax:*** no sntp

*Disables SNTP by changing the SNTP mode configuration to* **Disabled**.

For example, if the switch is running SNTP in Unicast mode with an SNTP servers as shown in figure 1-9, **no sntp** changes the SNTP configuration as shown below, and disables time synchronization on the switch.

```
HP Switch(config)# no sntp
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : disabled
  Poll Interval (sec) [720] : 720


  Priority SNTP Server Address                          Protocol Version
  -------- ------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                 7
  2        10.28.227.141                                4
  3        fe80::123%vlan10                             3
```

Even though the **Time Sync Mode** is set to **Sntp**, time synchronization is disabled because **no sntp** has disabled the **SNTP Mode** parameter.

**Figure 1-11. Example of Disabling Time Synchronization by Disabling the SNTP Mode**

# TimeP: Viewing, Selecting, and Configuring

| TimeP Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view the Timep time synchronization configuration | n/a | page 1-15 | page 1-17 | — |
| select Timep as the time synchronization method | TIMEP | page 1-14 | pages 1-18 ff. | — |
| disable time synchronization | timep | page 1-15 | page 1-20 | — |
| enable the Timep mode | Disabled | | | — |
| DHCP | — | page 1-15 | page 1-18 | — |
| manual | — | page 1-16 | page 1-19 | — |
| none/disabled | — | page 1-15 | page 1-21 | — |
| change the SNTP poll interval | 720 minutes | page 1-16 | page 1-20 | — |

**Table 1-2. Timep Parameters**

| SNTP Parameter | Operation |
|---|---|
| **Time Sync Method** | Used to select either TIMEP (the default), SNTP, or None as the time synchronization method. |
| **Timep Mode** | |
| **Disabled** | The Default. Timep does not operate, even if specified by the Menu interface **Time Sync Method** parameter or the CLI **timesync** command. |
| **DHCP** | When Timep is selected as the time synchronization method, the switch attempts to acquire a Timep server IP address via DHCP. If the switch receives a server address, it polls the server for updates according to the Timep poll interval. If the switch does not receive a Timep server IP address, it cannot perform time synchronization updates. |
| **Manual** | When Timep is selected as the time synchronization method, the switch attempts to poll the specified server for updates according to the Timep poll interval. If the switch fails to receive updates from the server, time synchronization updates do not occur. |
| **Server Address** | Used only when the **TimeP Mode** is set to **Manual**. Specifies the IP address of the TimeP server that the switch accesses for time synchronization updates. You can configure one server. |

## Menu: Viewing and Configuring TimeP

To View, Enable, and Modify the TimeP Protocol:

1. From the Main Menu, select:

   **2. Switch Configuration...**

   **1. System Information**

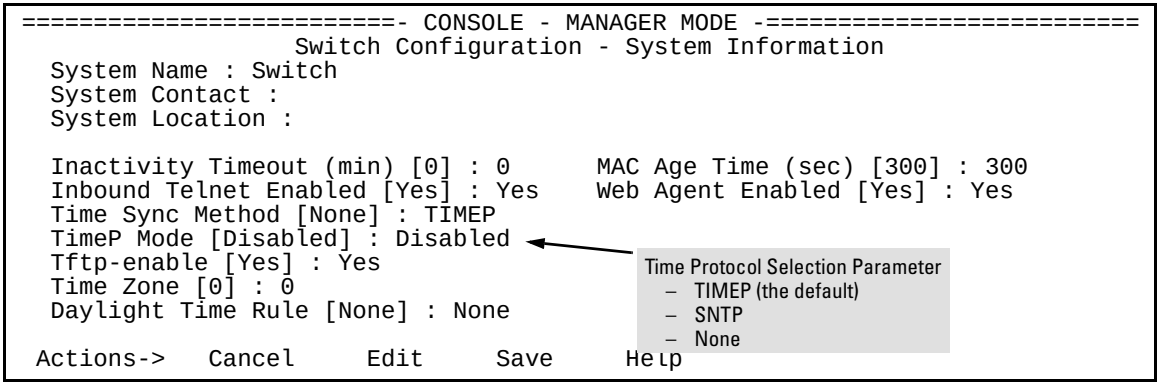



**Figure 1-12. The System Information Screen (Default Values)**

Press **[E]** (for **Edit**). The cursor moves to the **System Name** field.

2. Use [↓] to move the cursor to the **Time Sync Method** field.

3. If **TIMEP** is not already selected, use the Space bar to select **TIMEP**, then press ↓ once to display and move to the **TimeP Mode** field.
4. Do one of the following:
   - Use the Space bar to select the **DHCP** mode, then press ↓ to move the cursor to the **Poll Interval** field, and go to step 6.

```
Time Sync Method [None] : TIMEP
TimeP Mode [Disabled] : DHCP
Poll Interval (min) [720] : 720
Time Zone [0] : 0
Daylight Time Rule [None] : None
```

   - Use the Space bar to select the **Manual** mode.
     i. Press → to move the cursor to the **Server Address** field.
     ii. Enter the IP address of the TimeP server you want the switch to use for time synchronization.

     **Note:** This step replaces any previously configured TimeP server IP address.

     iii. Press → to move the cursor to the **Poll Interval** field, then go to step 6.
5. In the **Poll Interval** field, enter the time in minutes that you want for a TimeP Poll Interval.

Press **[Enter]** to return to the Actions line, **[S]** (for **Save**) to enter the new time protocol configuration in both the startup-config and running-config files.

## CLI: Viewing and Configuring TimeP

CLI Commands Described in this Section

| Command | Page |
|---|---|
| show timep | 1-17 |
| [no] timesync | 1-18, 1-18, 1-19, and 1-20 |
| ip timep | |
| dhcp | 1-18 |
| manual | 1-19 |
| server <*ip-addr*> | 1-19 |
| interval | 1-20 |
| no ip timep | 1-21 |

This section describes how to use the CLI to view, enable, and configure TimeP parameters.

## Viewing the Current TimeP Configuration

Using different **show** commands, you can display either the full TimeP configuration or a combined listing of all TimeP, SNTP, and VLAN IP addresses configured on the switch.

***Syntax:*** show timep

*This command lists both the time synchronization method (TimeP, SNTP, or None) and the TimeP configuration, even if SNTP is not the selected time protocol. (If the TimeP Mode is set to* **Disabled** *or* **DHCP**, *then the* **Server** *field does not appear.)*

For example, if you configure the switch with TimeP as the time synchronization method, then enable TimeP in DHCP mode with the default poll interval, **show timep** lists the following:

```
HP Switch(config)# show timep
 Timep Configuration
  Time Sync Mode: Timep
  TimeP Mode [Disabled] : DHCP    Server Address : 10.10.28.100
  Poll Interval (min) [720] : 720
```

**Figure 1-13. Example of TimeP Configuration When TimeP Is the Selected Time Synchronization Method**

If SNTP is the selected time synchronization method, **show timep** still lists the TimeP configuration even though it is not currently in use:

```
HP Switch(config)# show timep

 Timep Configuration

  Time Sync Mode: Sntp
  TimeP Mode [Disabled] : Manual     Server Address : 10.10.28.100
  Poll Interval (min) [720] : 720
```

Even though, in this example, SNTP is the current time synchronization method, the switch maintains the TimeP configuration.

**Figure 1-14. Example of TimeP Configuration When TimeP Is Not the Selected Time Synchronization Method**

***Syntax:*** show management

*This command can help you to easily examine and compare the IP addressing on the switch. It lists the IP addresses for all time servers configured on the switch, plus the IP addresses and default gateway for all VLANs configured on the switch.*

```
HP Switch(config)# show management
 Status and Counters - Management Address Information

  Time Server Address : 10.10.28.100

  Priority SNTP Server Address                          Protocol Version
  -------- ------------------------------------------- ----------------
  1        10.10..28.101                                3
  2        10.255.5.24                                  3
  3        fe80::123%vlan10                             3

  Default Gateway     : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + ------------------
  DEFAULT_VLAN 001279-88a100       | 10.30.248.184
  VLAN10       001279-88a100       | 10.0.10.17
```

**Figure 1-15. Example of Display Showing IP Addressing for All Configured Time Servers and VLANs**

## Configuring (Enabling or Disabling) the TimeP Mode

Enabling the TimeP mode means to configure it for either broadcast or unicast mode. Remember that to run TimeP as the switch's time synchronization protocol, you must also select TimeP as the time synchronization method by using the CLI timesync command (or the Menu interface **Time Sync Method** parameter).

***Syntax:*** timesync timep

*Selects TimeP as the time protocol.*

***Syntax:*** ip timep < dhcp | manual >

*Enables the selected TimeP mode.*

***Syntax:*** no ip timep

*Disables the TimeP mode.*

***Syntax:*** no timesync

*Disables the time protocol.*

**Enabling TimeP in DHCP Mode.** Because the switch provides a TimeP polling interval (default: 720 minutes), you need only these two commands for a minimal TimeP DHCP configuration:

***Syntax:*** timesync timep

*Selects TimeP as the time synchronization method.*

***Syntax:*** ip timep dhcp

*Configures DHCP as the TimeP mode.*

For example, suppose:

- Time synchronization is configured for SNTP.
- You want to:
  1. View the current time synchronization.
  2. Select TimeP as the time synchronization mode.
  3. Enable TimeP for DHCP mode.
  4. View the TimeP configuration.

The commands and output would appear as follows:

```
HP Switch(config)# show timep                    (1)
 Timep Configuration
  Time Sync Mode: Sntp
  TimeP Mode : Disabled

HP Switch(config)# timesync timep                (2)

HP Switch(config)# ip timep dhcp                 (3)

HP Switch(config)# show timep                    (4)
 Timep Configfuration
  Time Sync Mode: Timep
  TimeP Mode : DHCP    Poll Interval (min) : 720
```

**(1)** **show timep** displays the TimeP configuration and also shows that SNTP is the currently active time synchronization mode.

**(4)** **show timep** again displays the TimeP configuration and shows that TimeP is now the currently active time synchronization mode.

**Figure 1-16. Example of Enabling TimeP Operation in DHCP Mode**

**Enabling Timep in Manual Mode.** Like DHCP mode, configuring TimeP for **Manual** mode enables TimeP. However, for manual operation, you must also specify the IP address of the TimeP server. (The switch allows only one TimeP server.) To enable the TimeP protocol:

***Syntax:*** timesync timep

*Selects Timep.*

***Syntax:*** ip timep manual < *ip-addr* >

*Activates TimeP in Manual mode with a specified TimeP server.*

***Syntax:*** no ip timep

*Disables TimeP.*

**Note**

To change from one TimeP server to another, you must (1) use the **no ip timep** command to disable TimeP mode, and then reconfigure TimeP in Manual mode with the new server IP address.

For example, to select TimeP and configure it for manual operation using a TimeP server address of 10.28.227.141 and the default poll interval (720 minutes, assuming the TimeP poll interval is already set to the default):

```
HP Switch(config)# timesync timep
```

*Selects TimeP.*

```
HP Switch(config)# ip timep manual 10.28.227.141
```

*Activates TimeP in Manual mode.*

```
HP Switch(config)# timesync timep
HP Switch(config)# ip timep manual l0.28.227.l4l

HP Switch(config)# Show timep
 Timep Configuration

  Time Sync Mode: Timep
  TimeP Mode : Manual          Server Address : 10.28.227.141
  Poll Interval (min) : 720
```

**Figure 1-17. Example of Configuring Timep for Manual Operation**

**Changing the TimeP Poll Interval.** This command lets you specify how long the switch waits between time polling intervals. The default is 720 minutes and the range is 1 to 9999 minutes. (This parameter is separate from the poll interval parameter used for SNTP operation.)

***Syntax:*** ip timep < dhcp | manual > interval < 1 - 9999 >

For example, to change the poll interval to 60 minutes:

```
HP Switch(config)# ip timep interval 60
```

**Disabling Time Synchronization Without Changing the TimeP Configuration.** The recommended method for disabling time synchronization is to use the **timesync** command. This halts time synchronization without changing your TimeP configuration.

***Syntax:*** no timesync

*Disables time synchronization by changing the* **Time Sync Mode** *configuration to* **Disabled**.

For example, suppose TimeP is running as the switch's time synchronization protocol, with **DHCP** as the TimeP mode, and the factory-default polling interval. You would halt time synchronization with this command:

```
HP Switch(config)# no timesync
```

If you then viewed the TimeP configuration, you would see the following:

```
HP Switch(config)# show timep
 Timep Configuration
  Time Sync Mode: Disabled
  TimeP Mode : DHCP    Po11 Interval (min) : 720
```

**Figure 1-18. Example of TimeP with Time Sychronization Disabled**

**Disabling the TimeP Mode.** Disabling the TimeP mode means to configure it as disabled. (Disabling TimeP prevents the switch from using it as the time synchronization protocol, even if it is the selected **Time Sync Method** option.)

***Syntax:*** no ip timep

*Disables TimeP by changing the TimeP mode configuration to* **Disabled**.

For example, if the switch is running TimeP in DHCP mode, **no ip timep** changes the TimeP configuration as shown below, and disables time synchronization.

```
HP Switch(config)# no ip timep

HP Switch(config)# show timep
 Timep Configuration
  Time Sync Mode: Timep
  TimeP Mode : Disabled
```

Even though the Time Sync Mode is set to Timep, time synchronization is disabled because no ip timep has disabled the TimeP Mode parameter.

**Figure 1-19. Example of Disabling Time Synchronization by Disabling the TimeP Mode Parameter**

# SNTP Unicast Time Polling with Multiple SNTP Servers

When running SNTP unicast time polling as the time synchronization method, the switch requests a time update from the server you configured with either the Server Address parameter in the menu interface, or the primary server in a list of up to three SNTP servers configured using the CLI. If the switch does not receive a response from the primary server after three consecutive polling intervals, the switch tries the next server (if any) in the list. If the switch tries all servers in the list without success, it sends an error message to the Event Log and reschedules to try the address list again after the configured **Poll Interval** time has expired.

## Displaying All SNTP Server Addresses Configured on the Switch

The System Information screen in the menu interface displays only one SNTP server address, even if the switch is configured for two or three servers. The CLI **show management** command displays all configured SNTP servers on the switch.

```
HP Switch(config)# show management

 Status and Counters - Management Address Information

  Time Server Address : fe80::215:60ff:fe7a:adc0%vlan10

  Priority SNTP Server Address                          Protocol Version
  -------- ------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                 7
  2        10.255.5.24                                  3
  3        fe80::123%vlan10                             3


  Default Gateway     : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + ------------------
  DEFAULT_VLAN 001279-88a100       | Disabled
  VLAN10       001279-88a100       | 10.0.10.17
```

**Figure 1-20. Example of How To List All SNTP Servers Configured on the Switch**

## Adding and Deleting SNTP Server Addresses

**Adding Addresses.** As mentioned earlier, you can configure one SNTP server address using either the Menu interface or the CLI. To configure a second and third address, you must use the CLI. To configure the remaining two addresses, you would do the following:

```
HP Switch(config)# sntp server 2001:db8::215:60ff:fe79:8980
HP Switch(config)# sntp server 10.255.5.24
```

**Figure 1-21. Example of Creating Additional SNTP Server Addresses with the CLI**

**Note**

If there are already three SNTP server addresses configured on the switch, and you want to use the CLI to replace one of the existing addresses with a new one, you must delete the unwanted address before you configure the new one.

**Deleting Addresses.** To delete an address, you must use the CLI. If there are multiple addresses and you delete one of them, the switch re-orders the address priority.

***Syntax:*** no sntp server < *ip-addr* >

For example, to delete the primary address in the above example (and automatically convert the secondary address to primary):

```
HP Switch(config)# no sntp server 10.28.227.141
```

## Menu: Operation with Multiple SNTP Server Addresses Configured

When you use the Menu interface to configure an SNTP server IP address, the new address writes over the current primary address, if one is configured.

# SNTP Messages in the Event Log

If an SNTP time change of more than three seconds occurs, the switch's event log records the change. SNTP time changes of less than three seconds do not appear in the Event Log.

# Port Status and Configuration

## Overview

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including

- Enable/Disable
- Mode (speed and duplex)
- Flow Control
- Broadcast Limit
- Jumbo Packets
- Friendly Port Names
- Uni-directional Link Detection (UDLD)

## Viewing Port Status and Configuring Port Parameters

**Port Status and Configuration Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port status | n/a | page 2-2 | page 2-6 | page 2-21 |
| viewing transceiver status | n/a | n/a | page 2-13 | page 2-21 |
| configuring ports | | page 2-5 | page 2-14 | page 2-21 |
| configuring auto-mdix | | | page 2-18 | |

**Note On Connecting Transceivers to Fixed-Configuration Devices**

If the switch either fails to show a link between an installed transceiver and another device, or demonstrates errors or other unexpected behavior on the link, check the port configuration on both devices for a speed and/or duplex (mode) mismatch.

- To check the mode setting for a port on the switch, use either the Port Status screen in the menu interface (page 2-2) or **show interfaces brief** in the CLI (page 2-6).

To display information about the transceivers installed on a switch, enter the **show tech transceivers** command in the CLI (page 2-13).

## Menu: Port Status and Configuration

From the menu interface, you can view and change the port configuration.

**Using the Menu To View Port Configuration.** The menu interface displays the configuration for ports and (if configured) any trunk groups.

From the Main Menu, select:

**1. Status and Counters**
**4. Port Status**

```
=========================- CONSOLE - MANAGER MODE -=========================
                       Status and Counters - Port Status

                    Intrusion                                  MDI   Flow   Bcast
  Port     Type       Alert    Enabled  Status     Mode      Mode   Ctrl   Limit
  -----  ---------  --------- -------  ------  ----------  -----  -----  ------
  1      100/1000T  No         Yes      Down    100FDx      Auto  off    0
  2      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  3      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  4      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  5      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  6      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  7      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  8      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  9      100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  10     100/1000T  No         Yes      Down    1000FDx     Auto  off    0
  11     100/1000T  No         Yes      Down    1000FDx     Auto  off    0

 Actions->   Back     Intrusion log     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 2-1. Example of a Switch Port Status Screen**

### Port Type

The port Type field represents the IEEE or other industry protocol in operation on that port. For example, 1000Base-SX is a gigabit protocol for gigabit operation over fiber optic cable.

## Status of Ports

A port can be enabled or disabled:

- **Yes**: Enabled, the default. This indicates the port is ready for a network connection.
- **No**: Disabled, the port will not operate, even if properly connected to a network. Use the setting, for example, to shut the port down for diagnostic purposes or while you are making topology changes.

The status of a port can be up or down (Read-only):

**Up**: The port senses a link beat.

**Down**: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, see the *Installation and Getting Started Guide* for your switch, or refer to Appendix C, "Troubleshooting" (in this manual).

## Flow Control

With the port mode set to Auto (the default) and flow control on (enabled), the switch negotiates flow control on the indicated port. If the port mode is not set to Auto, or if flow control is off (disabled) on the port, then flow control is not used. Flow control must be enabled on both ends of a link.

- **On**: Enabled. The port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.
- Off: Disabled (default).The port does not generate flow control packets, and drops any flow control packets it receives.

## Broadcast Limit

The broadcast limit specifies the percentage of the theoretical maximum network bandwidth that can be used for broadcast and multicast traffic. Any broadcast or multicast traffic exceeding that limit will be dropped. Zero (0) means the feature is disabled.

The **broadcast-limit** command operates at the port context level to set the broadcast limit for a port on a switch.

**Note**

This feature is not appropriate for networks that require high levels of IPX or RIP broadcast traffic.

## Modes

The mode is the port's speed and duplex (date transfer operation) setting. Table 2-1 shows possible modes available, depending on the port type (copper or fiber) and port speed.

**Table 2-1. Supported Modes**

| Mode | Speed and Duplex Settings |
|---|---|
| Auto-MDIX | Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI). To see what the switch negotiates for the Auto setting, use the CLI **show interfaces brief** command or the menu commands "**1. Status and Counters**", "**3. Port Status**".<br>This features applies only to copper port switches using twisted-pair copper Ethernet cables. |
| MDI | Sets the port to connect with a PC using a crossover cable (Manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables). |
| MDIX | Sets the port to connect with a PC using a straight-through cable (Manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables). |
| Auto-10 | Allows the port to negotiate between half-duplex (HDx) and full-duplex (FDx) while keeping speed at 10Mbps. Also negotiates flow control (enabled or disabled). HP recommends Auto-10 for links between 10/100 auto-sensing ports connected with Cat 3 cabling. (Cat 5 cabling is required for 100 Mbps links.) |
| Auto-100 | Uses 100 Mbps and negotiates with the port at the other end of the link for other port operation features. |
| Auto-10-100 | Allows the port to establish a link with the port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting. |
| Auto-1000 | Uses 1000 Mbps and negotiates with the port at the other end of the link for other port operation features. |
| 10HDx | Uses 10 Mbps, Half-Duplex |
| 100HDx | Uses 100 Mbps, Half-Duplex |
| 10FDX | Uses 10 Mbps, Full-Duplex |
| 100FDx | Uses 100 Mbps, Full-Duplex |
| 1000FDx | Uses 1000 Mbps, Full-Duplex |
| 10 GbE FDx | Uses 10 Gigabits/sec Full-Duplex |

Tables 2-2 and 2-3 display the protocols and modes supported for copper ports and fiber optic ports, respectively.

**Table 2-2. Protocols and Modes Supported for Copper Ports**

| 10/100 Mbps | | Gigabit | | 10 Gigabit | |
|---|---|---|---|---|---|
| 10/100 TX | | 10/100/1000-T | | 10GBASE-CX4 | |
| **Modes** | **Settings** | **Modes** | **Settings** | **Modes** | **Settings** |
| Auto<br>10HDx<br>100HDx<br>10FDx<br>100FDx<br>Auto-10 | 100FDx<br>10HDx<br>100HDx<br>10FDx<br>100FDX<br>10FDX | Auto<br>Auto-10<br>Auto-100<br>Auto-10-100<br>Auto-1000<br>10HDx<br>100HDX<br>1000FDx | 1000FDx<br>10HDx<br>100FDx<br>100FDx<br>1000FDx<br>10HDx<br>100HDx<br>1000FDx | Auto | 10 Gigabit FDx |

**Table 2-3. Protocols and Modes Supported for Fiber Optic Ports**

| | 100 Mbps | Gigabit | 10 Gigabit |
|---|---|---|---|
| **Protocols** | 100BASE-FX<br>100BASE-BX10 | 1000BASE-SX<br>1000BASE-LX<br>1000BASE-BX10<br>1000BASE-LH | 10GBASE-SR<br>10GBASE-LR<br>10GBASE-LRM |
| **Modes** | 100HDx<br>100FDx | Auto<br>1000FDx | Auto |

## Configuring Ports

You can configure and view the port settings by using the menu.

**Note**

The menu interface uses the same screen for configuring both individual ports and port trunk groups. For information on port trunk groups, refer to Chapter 4, “Port Trunking” .

1. From the Main Menu, Select:
   **2. Switch Configuration...**
   **2. Port/Trunk Settings**

An example of the Menu display is shown below.

```
============================- TELNET - MANAGER MODE -==============
                    Switch Configuration - Port/Trunk Settings

  Port    Type       Enabled      Mode       Flow Ctrl  Group  Type
  ----  --------- + -------  ------------  ---------  -----  -----
  1     1000T     | Yes      Auto-10-100   Disable
  2     1000T     | Yes      Auto-10-100   Disable
  3     1000T     | Yes      Auto          Disable
  4     1000T     | Yes      Auto-1000     Disable
  5     1000T     | Yes      10HDx         Disable
  6     1000T     | Yes      10FDx         Disable
  7     1000T     | Yes      100FDx        Disable     Trk1  Trunk
  8     1000T     | Yes      Auto          Disable     Trk2  Trunk

 Actions->   Cancel     Edit     Save     Help
```

**Figure 2-2. Example of Port/Trunk Settings with a Trunk Group Configured**

2. Press **[E]** (for Edit). The cursor moves to the **Enabled** field for the first port.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press **[Enter],** then press **[S]** (for **Save**).

## CLI: Viewing Port Status and Configuring Port Parameters

From the CLI, you can configure and view all port parameter settings and view all port status indicators.

### Port Status and Configuration Commands


| | |
|---|---|
| show interfaces brief | page 2-7 |
| show interfaces config | page 2-7 |
| show interfaces port-utilization | page 2-12 |
| show tech transceivers | page 2-13 |
| interface | page 2-14 |
| disable/enable | page 2-14 |
| speed-duplex | page 2-14 |
| flow-control | page 2-15 |
| broadcast-limit | page 2-17 |
| auto-mdix | page 2-18 |

## Viewing Port Status and Configuration

Use the following commands to display port status and configuration data.

***Syntax:*** show interfaces [ brief | config | < *port-list* >]

**brief:** *Lists the current operating status for all ports on the switch.*

**config:** *Lists a subset of configuration data for all ports on the switch; that is, for each port, the display shows whether the port is enabled, the operating mode, and whether it is configured for flow control.*

**< *port-list* >:** Shows a summary of network traffic handled by the specified ports.

An example of the **show interfaces brief** command is shown below.

```
HP Switch(config)# show interfaces brief
Status and Counters - Port Status

                  | Intrusion                              MDI   Flow  Bcast
  Port  Type      | Alert     Enabled Status Mode          Mode  Ctrl  Limit
  ----- --------- + --------- ------- ------ ----------    ----- ----- ------
  1     100/1000T | No        Yes     Down   Auto-10-100   Auto  off   0
  2     100/1000T | No        Yes     Down   1000FDx       Auto  off   0
  3     100/1000T | No        Yes     Down   1000FDx       Auto  off   0
  4     100/1000T | No        Yes     Down   1000FDx       Auto  off   0
  5     100/1000T | No        Yes     Down   1000FDx       Auto  off   0
  6     100/1000T | No        Yes     Down   1000FDx       Auto  off   0
```

**Figure 2-3. Example of show interfaces brief Command Listing**

Use the **show interfaces config** command to view the port settings, as shown below.

```
HP Switch(config)# show interfaces config

 Port Settings

  Port  Type      | Enabled Mode         Flow Ctrl MDI
  ----- --------- + ------- ------------ --------- ----
  1     100/1000T   Yes     Auto-10-100  Disable   Auto
  2     100/1000T   Yes     Auto         Disable   Auto
  3     100/1000T   Yes     Auto         Disable   Auto
  4     100/1000T   Yes     Auto         Disable   Auto
  5     100/1000T   Yes     Auto         Disable   Auto
```

**Figure 2-4. Example of a show interfaces config Command Listing**

The **display** option can be used to initiate the dynamic update of the **show interfaces** command with the output being the same as the **show interfaces** command. When using the **display** option in the CLI, the information stays on the screen and is updated every 3 seconds, as occurs with the display using the menu feature. The update is terminated with Cntl-C.

You can use the arrow keys to scroll through the screen when the output does not fit in one screen.

***Syntax:*** show int display

*Initiates the dynamic update of a command. The output is the same as the equivalent "***show***" command.The information is updated every 3 seconds.*

***Note****: Select "Back" to exit the display.*

For example:

```
HP Switch# show int display
```

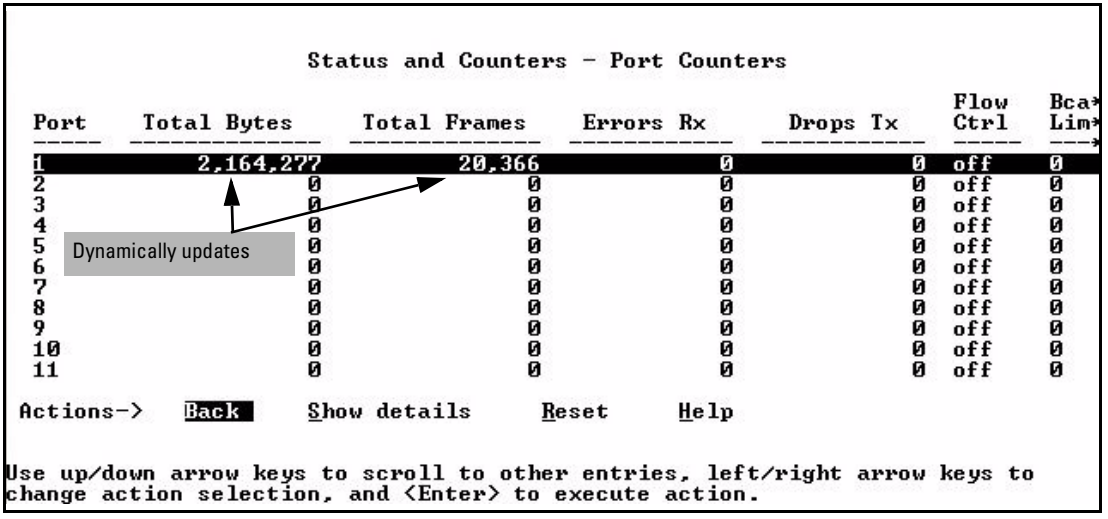



**Figure 2-5. Example of show int display Command with Dynamically Updating Output**

## Customizing the Show Interfaces Command

You can create **show** commands displaying the information that you want to see in any order you want by using the **custom** option.

***Syntax:*** show interfaces custom [port-list] column-list

*Select the information that you want to display. Parameters include:*

- *port name*
- *type*
- *vlan*
- *intrusion*
- *enabled*
- *status*
- *speed*
- *mdi*
- *flow*

Columns supported are:

| Parameter Column | Displays | Examples |
|---|---|---|
| port | Port identifier | 2 |
| type | Port type | 100/1000T |
| status | Port status | up or down |
| speed | Connection speed and duplex | 1000FDX |
| mode | Configured mode | auto, auto-100, 100FDX |
| mdi | MDI mode | auto, MDIX |
| flow | Flow control | on or off |
| name | Friendly port name | |
| vlanid | The vlan id this port belongs to, or "tagged" if it belongs to more than one vlan | 4<br>tagged |
| enabled | port is or is not enabled | yes or no<br>intrusion |
| intrusion | Intrusion alert status | no |
| bcast | Broadcast limit | 0 |

```
HP Switch(config)# show int custom 1-4 port name:4 type vlan intrusion speed
enabled mdi

 Status and Counters - Custom Port Status

                                  Intrusion
  Port Name       Type       VLAN  Alert     Speed   Enabled MDI-mode
  ---- ---------- ---------- ----- --------- ------- ------- --------
  1    Acco       10/100T    1     No        100FDx  Yes     Auto
  2    Huma       10/100T    1     No        100FDx  Yes     Auto
  3    Deve       10/100T    1     No        100FDx  Yes     Auto
  4    Labl       10/100T    1     No        100FDx  Yes     Auto
```

**Figure 2-6. Example of the Custom show interfaces Command**

You can specify the column width by entering a colon after the column name, then indicating the number of characters to display. In Figure 2-6 the Name column only displays the first four characters of the name. All remaining characters are truncated.

**Note**

Each field has an fixed minimum width to be displayed. If you specify a field width smaller than the minimum width, the information is displayed at the minimum width. For example, if the minimum width for the Name field is 4 characters and you specify Name:2, the Name field displays 4 characters.

Parameters can be entered in any order. There is a limit of 80 characters per line; if you exceed this limit an error displays.

## Error Messages

| Error | Error Message |
|---|---|
| Requesting too many fields (total characters exceeds 80) | Total length of selected data exceeds one line |
| Field name is misspelled | Invalid input: <input> |
| Mistake in specifying the port list | Module not present for port or invalid port: <input> |
| The port list is not specified | Incomplete input: custom |

## Note on Using Pattern Matching with the "Show Interfaces Custom" Command

If you have included a pattern matching command to search for a field in the output of the **show int custom** command and the **show int custom** command produces an error, the error message may not be visible and the output is empty. For example, if you enter a command that produces an error (vlan is misspelled) with the pattern matching **include** option:

```
HP Switch(config)# show int custom 1-3 name vlun |
                    include vlan1
```

the output may be empty. It is advisable to try the **show int custom** command first to ensure there is output, and then enter the command again with the pattern matching option.

```
HP Switch(config)# show int custom 1-4 port name:4 type vlan intrusion speed
enabled mdi

 Status and Counters - Custom Port Status

                                  Intrusion
  Port Name       Type       VLAN  Alert     Speed   Enabled MDI-mode
  ---- ---------- ---------- ----- --------- ------- ------- --------
  1    Acco       100/1000T  1     No        1000FDx Yes     Auto
  2    Huma       100/1000T  1     No        1000FDx Yes     Auto
  3    Deve       100/1000T  1     No        1000FDx Yes     Auto
  4    Labl       100/1000T  1     No        1000FDx Yes     Auto
```

**Figure 2-7. Example of the Custom show interfaces Command**

You can specify the column width by entering a colon after the column name, then indicating the number of characters to display. In Figure 2-6 the Name column only displays the first four characters of the name. All remaining characters are truncated.

**Note**

Each field has an fixed minimum width to be displayed. If you specify a field width smaller than the minimum width, the information is displayed at the minimum width. For example, if the minimum width for the Name field is 4 characters and you specify Name:2, the Name field displays 4 characters.

Parameters can be entered in any order. There is a limit of 80 characters per line; if you exceed this limit an error displays.

## Error Messages

| Error | Error Message |
|---|---|
| Requesting too many fields (total characters exceeds 80) | Total length of selected data exceeds one line |
| Field name is misspelled | Invalid input: <input> |
| Mistake in specifying the port list | Module not present for port or invalid port: <input> |
| The port list is not specified | Incomplete input: custom |

## Note on Using Pattern Matching with the "Show Interfaces Custom" Command

If you have included a pattern matching command to search for a field in the output of the **show int custom** command and the **show int custom** command produces an error, the error message may not be visible and the output is empty. For example, if you enter a command that produces an error (vlan is misspelled) with the pattern matching **include** option:

```
HP Switch(config)# show int custom 1-3 name vlun |
                  include vlan1
```

the output may be empty. It is advisable to try the **show int custom** command first to ensure there is output, and then enter the command again with the pattern matching option.

# Viewing Port Utilization Statistics

Use the **show interface port-utilization** command to view a real-time rate display for all ports on the switch. The following shows a sample output from this command.

```
HP Switch(config)# show interfaces port-utilization
 Status and Counters - Port Utilization
                                Rx                          Tx
 Port      Mode     | --------------------------- | ---------------------------
                    | Kbits/sec   Pkts/sec  Util  | Kbits/sec  Pkts/sec   Util
 --------- -------- + ---------- ---------- ----- + ---------- ---------- -----
 1         1000FDx  | 0          0          0     | 0          0          0
 2         1000FDx  | 0          0          0     | 0          0          0
 3         1000FDx  | 0          0          0     | 0          0          0
 4         1000FDx  | 0          0          0     | 0          0          0
 5         1000FDx  | 0          0          0     | 0          0          0
 6         1000FDx  | 0          0          0     | 0          0          0
 7         100FDx   | 624        86         00.62 | 496        0          00.49
```

**Figure 2-8. Example of a Show Interface Port-Utilization Command Listing**

Operating Notes:

- For each port on the switch, the command provides a real-time display of the rate at which data is received (Rx) and transmitted (Tx) in terms of kilobits per second (KBits/s), number of packets per second (Pkts/s), and utilization (Util) expressed as a percentage of the total bandwidth available.
- The **show interfaces** <port-list> command can be used to display the current link status and the port rate average over a 5 minute period. Port rates are shown in bits per second (bps) for ports up to 1 Gigabit; for 10 Gigabit ports, port rates are shown in kilobits per second (Kbps).

## Viewing Transceiver Status

The **show tech transceivers** command allows you to:

- Remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its port.
- Display real-time status information about all installed transceivers, including non-operational transceivers.Figure 2-9 shows sample output from the **show tech transceivers** command.

```
HP Switch# show tech transceivers
Transceiver Technical Information:
 Port # |   Type    | Prod # | Serial #         | Part #
 -------+-----------+--------+------------------+----------
 21     | 1000SX    | J4858B | CN605MP23K       |
 22     | 1000LX    | J4859C | H117E7X          | 2157-2345
```

**Figure 2-9. Example of Show Tech Transceivers Command**

Operating Notes:

- The following information is displayed for each installed transceiver:
  - Port number on which transceiver is installed.
  - Type of transceiver.
  - Product number—Includes revision letter, such as A, B, or C. If no revision letter follows a product number, this means that no revision is available for the transceiver.
  - Part number—Allows you to determine the manufacturer for a specified transceiver and revision number.
- For a non-HP installed transceiver (see line 23 Figure 2-9), no transceiver type, product number, or part information is displayed. In the Serial Number field, **non-operational** is displayed instead of a serial number.

- The following error messages may be displayed for a non-operational transceiver:
  - `Unsupported Transceiver. (SelfTest Err#060) Check: www.hp.com/rnd/device_help/2_inform for more info.`
  - `This switch only supports revision B and above transceivers. Check: www.hp.com/rnd/device_help/2_inform for more info.`
  - `Self test failure.`
  - `Transceiver type not supported in this port.`
  - `Transceiver type not supported in this software version.`
  - `Not an HP Transceiver. Please go to: www.hp.com/rnd/device_help/2_inform for more info.`

## Enabling or Disabling Ports and Configuring Port Mode

You can configure one or more of the following port parameters.

***Syntax:*** [no] interface < *port-list* >

[< disable | enable >]

*Disables or enables the port for network traffic. Does not use the* **no** *form of the command. (Default:* **enable**.*)*

[speed-duplex < auto-10 |10-full | 10-half | 100-full | 100-half |1000-full |auto| auto 100 | auto-1000 | auto 10-100 >]

*Specifies the port's data transfer speed and mode. Does not use the* **no** *form of the command. (Default:* **auto**.*)*

Note that in the above syntax you can substitute an "**int**" for "**interface**"; that is: **int < *port-list* >**.

The 10/100 auto-negotiation feature allows a port to establish a link with a port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting.

For example, to configure port 5 for auto-10-100, enter this command:

```
HP Switch(config)# int 5 speed-duplex auto-10-100
```

To configure ports 1 through 3 and port 6 for 100Mbps full-duplex, you would enter these commands:

```
HP Switch(config)# int 1-3,6 speed-duplex 100-full
```

Similarly, to configure a single port with the above command settings, you could either enter the same command with only the one port identified, or go to the *context level* for that port and then enter the command. For example, to enter the context level for port 6 and then configure that port for 100FDx:

```
HP Switch(config)# int e 6
HP Switch(eth-6)# speed-duplex 100-full
```

If port 8 was disabled, and you wanted to enable it and configure it for 100FDx with flow-control active, you could do so with either of the following command sets.

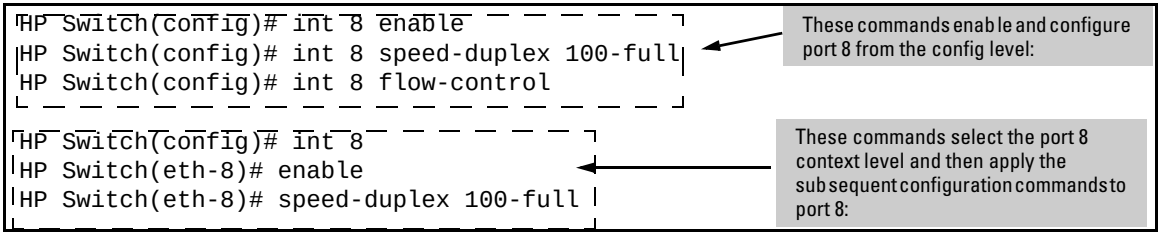



**Figure 2-10. Examples of Two Methods for Changing a Port Configuration**

Refer to "Enabling or Disabling Flow Control" on page 2-15 for more on flow control.

## Enabling or Disabling Flow Control

**Note**

You must enable flow control on both ports in a given link. Otherwise, flow control does not operate on the link, and appears as **Off** in the **show interfaces brief** port listing, even if flow control is configured as enabled on the port in the switch. (Refer to Figure 2-3 on page 2-7.) Also, the port (speed-duplex) mode must be set to **Auto** (the default).

To disable flow control on some ports, while leaving it enabled on other ports, just disable it on the individual ports you want to exclude.

***Syntax:*** [ no ]interface < *port-list* > flow-control

*Enables or disables flow control packets on the port. The "***no***" form of the command disables flow control on the individual ports. (Default: Disabled.)*

For example, suppose that:

1. You want to enable flow control on ports 7-11.
2. Later, you decide to disable flow control on port 11.

3. As a final step, you want to disable flow control on all ports.

Assuming that flow control is currently disabled on the switch, you would use these commands:

```
HP Switch(config)# int 7-10 flow-control
HP Switch(config)# show int brief

 Status and Counters - Port Status

                   | Intrusion                              MDI   Flow  Bcast
  Port    Type     | Alert     Enabled Status Mode          Mode  Ctrl  Limit
  ------- -------- + --------- ------- ------ ----------- ----- ----- ------
  1       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  2       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  3       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  4       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  5       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  6       100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  7-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  8-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  9-Trk2  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  10-Trk2 100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  11      100/1000T | No        Yes     Up     1000FDx     Auto  on    0
```

**Figure 2-11. Example of Configuring Flow Control for a Series of Ports**

```
HP Switch(config)# no int 11 flow-control
HP Switch(config)# show int brief

 Status and Counters - Port Status

                   | Intrusion                              MDI   Flow  Bcast
  Port    Type     | Alert     Enabled Status Mode          Mode  Ctrl  Limit
  ------- -------- + --------- ------- ------ ----------- ----- ----- ------
  1       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  2       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  3       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  4       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  5       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  6       100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  7-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  8-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  9-Trk2  100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  10-Trk2 100/1000T | No        Yes     Up     1000FDx     Auto  on    0
  11      100/1000T | No        Yes     Up     1000FDx     Auto  off   0
```

Disables per-port flow control on port 11.

**Figure 2-12. Example Continued from Figure 2-11**

```
HP Switch(config)# no int 7-10 flow-control
HP Switch(config)# show int brief

 Status and Counters - Port Status

                   | Intrusion                              MDI   Flow  Bcast
  Port    Type     | Alert     Enabled Status Mode          Mode  Ctrl  Limit
  ------- -------- + --------- ------- ------ ----------- ----- ----- ------
  1       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  2       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  3       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  4       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  5       100/1000T | No        Yes     Down   1000FDx     Auto  off   0
  6       100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  7-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  8-Trk1  100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  9-Trk2  100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  10-Trk2 100/1000T | No        Yes     Up     1000FDx     Auto  off   0
  11      100/1000T | No        Yes     Up     1000FDx     Auto  off   0
```

**Figure 2-13. Example Continued from Figure 2-12**

## Configuring a Broadcast Limit on the Switch

Broadcast-Limit on switches covered in this guide is configured on a per-port basis. You must be at the port context level for this command to work, for example:

```
HP Switch(config)#int 1
HP Switch(int 1)# broadcast-limit 1
```

**Broadcast-Limit.**

***Syntax:*** broadcast-limit <0-99>

*Enables or disables broadcast limiting for outbound broadcasts on a selected port on the switch. The value selected is the percentage of traffic allowed, for example,* **broadcast-limit 5** *allows 5% of the maximum amount of traffic for that port. A value of zero disables broadcast limiting for that port.*

***Note:*** *You must switch to port context level before issuing the* **broadcast-limit** *command.*

***Note:*** *This feature is not appropriate for networks requiring high levels of IPX or RIP broadcast traffic.*

***Syntax:*** show config

*Displays the startup-config file. The broadcast limit setting appears here if enabled and saved to the startup-config file.*

***Syntax:*** show running-config

*Displays the running-config file. The broadcast limit setting appears here if enabled. If the setting is not also saved to the startup-config file, rebooting the switch returns broadcast limit to the setting currently in the startup-config file.*

For example, the following command enables broadcast limiting of 1 percent of the traffic rate on the selected port on the switch:

```
HP Switch(int 1)# broadcast-limit 1
```

For a one Gbps port this results in a broadcast traffic rate of ten Mbps.

## Configuring Auto-MDIX

Copper ports on the switch can automatically detect the type of cable configuration (MDI or MDI-X) on a connected device and adjust to operate appropriately.

This means you can use a “straight-through” twisted-pair cable or a “crossover” twisted-pair cable for any of the connections—the port makes the necessary adjustments to accommodate either one for correct operation. The following port types on your switch support the IEEE 802.3ab standard, which includes the “Auto MDI/MDI-X” feature:

- 10/100-TX al module ports
- 100/1000-T al module ports
- 10/100/1000-T al module ports

Using the above ports:

- If you connect a copper port using a straight-through cable on a switch to a port on another switch or hub that uses MDI-X ports, the switch port automatically operates as an MDI port.
- If you connect a copper port using a straight-through cable on a switch to a port on an end node, such as a server or PC, that uses MDI ports, the switch port automatically operates as an MDI-X port.

Auto-MDIX was developed for auto-negotiating devices, and was shared with the IEEE for the development of the IEEE 802.3ab standard. Auto-MDIX and the IEEE 802.3ab Auto MDI/MID-X feature are completely compatible. Additionally, Auto-MDIX supports operation in forced speed and duplex modes.

If you want more information on this subject please refer to the *IEEE 802.3ab Standard Reference*.

For more information on MDI-X, refer to the appendix titled "Switch Ports and Network Cables" in the *Installation and Getting Started Guide* for your switch.

**Manual Override.** If you require control over the MDI/MDI-X feature you can set the switch to either of two non-default modes:

- Manual MDI
- Manual MDI-X

Table shows the cabling requirements for the MDI/MDI-X settings.Cable Types for Auto and Manual MDI/MDI-X Settings

| Setting | MDI/MDI-X Device Type | |
|---|---|---|
| | PC or Other MDI Device Type | Switch, Hub, or Other MDI-X Device |
| Manual MDI | Crossover Cable | Straight-Through Cable |
| Manual MDI-X | Straight-Through Cable | Crossover Cable |
| Auto-MDI-X (The Default) | Either Crossover or Straight-Through Cable | |

The Auto-MDIX features apply only to copper port switches using twisted-pair copper Ethernet cables.

***Syntax:*** interface < *port-list* > mdix-mode < automdix | mdi | mdix >

**automdix** *is the automatic, default setting. This configures the port for automatic detection of the cable (either straight-through or crossover).*

**mdi** *is the manual mode setting that configures the port for connecting to either a PC or other MDI device with a crossover cable, or to a switch, hub, or other MDI-X device with a straight-through cable.*

**mdix** *is the manual mode setting that configures the port for connecting to either a switch, hub, or other MDI-X device with a crossover cable, or to a PC or other MDI device with a straight-through cable.*

***Syntax:*** show interfaces config

*Lists the current per-port Auto/MDI/MDI-X configuration.*

***Syntax:*** show interfaces brief

*Where a port is linked to another device, this command lists the MDI mode the port is currently using. In the case of ports configured for* **Auto** (**automdix**), *the MDI mode appears as either* **MDI** *or* **MDIX**, *depending upon which option the port has negotiated with the device on the other end of the link. In the case of ports configured for* **MDI** *or* **MDIX**, *the mode listed in this display matches the configured setting. If the link to another device was up, but has gone down, this command shows the last operating MDI mode the port was using. If a port on a given switch has not detected a link to another device since the last reboot, this command lists the MDI mode to which the port is currently configured.*

For example, **show interfaces config** displays the following data when port 1 is configured for **auto-mdix**, port 2 is configured for **mdi**, and port 3 is configured for **mdix**.

```
HP Switch(config)# show interfaces config

 Port Settings
  Port    Type      | Enabled Mode         Flow Ctrl MDI
  ------- --------- + ------- ------------ ---------┌---- ┐
  1       100/1000T | Yes     Auto         Disable  |Auto |
  2       100/1000T | Yes     Auto         Disable  |MDI  |
  3       100/1000T | Yes     Auto         Disable  |MDIX |
  4       100/1000T | Yes     Auto         Disable  |Auto |
  5       100/1000T | Yes     Auto         Disable  └Auto ┘
```

Per-Port MDI Configuration

**Figure 2-14. Example of Displaying the Current MDI Configuration**

```
HP Switch(config)# show int brief

 Status and Counters - Port Status

                    | Intrusion                          ┌ MDI  ┐ Flow  Bcast
  Port    Type      | Alert     Enabled Status Mode      | Mode | Ctrl  Limit
  ------- --------- + --------- ------- ------ ---------┤ -----┤ ----- ------
  1       100/1000T | No        Yes     Down   1000FDx   | MDIX | off   0
  2       100/1000T | No        Yes     Down   100FDx    | MDI  | off   0
  3       100/1000T | No        Yes     Down   100FDx    | MDIX | off   0
  4       100/1000T | No        Yes     Down   1000FDx   | Auto | off   0
  5       100/1000T | No        Yes     Down   1000FDx   | Auto | off   0
  6       100/1000T | No        Yes     Up     1000FDx   └ Auto ┘ off   0
```

Per-Port MDI Operating Mode

**Figure 2-15. Example of Displaying the Current MDI Operating Mode**

### Web: Viewing Port Status and Configuring Port Parameters

In the web browser interface:

1. Click on the **Configuration** tab.
2. Click on **[Port Configuration]**.
3. Select the ports you want to modify and click on **[Modify Selected Ports]**.
4. After you make the desired changes, click on **[Apply Settings]**.

Note that the web browser interface displays an existing port trunk group. However, to configure a port trunk group, you must use the CLI or the menu interface. For more on this topic, refer to Chapter 4, “Port Trunking” .

## Jumbo Packets

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| display VLAN jumbo status | n/a | — | 2-23 | — |
| configure jumbo VLANs | Disabled | — | 2-25 | — |

The *Maximum Transmission Unit* (MTU) is the maximum size IP packet the switch can receive for Layer 2 packets inbound on a port. The switch drops any inbound packets larger than the MTU allowed on the port. On ports operating at 10 Mbps or 100 Mbps, the MTU is fixed at 1522 bytes. However, ports operating at 1 Gbps or 10 Gbps speeds accept forward packets of up to 9220 bytes (including four bytes for a VLAN tag) when configured for jumbo traffic. In switches covered in this guide, you can enable inbound jumbo packets on a per-VLAN basis. That is, on a VLAN configured for jumbo traffic, all ports belonging to that VLAN and *operating* at 1 Gbps or 10 Gbps allow inbound jumbo packets of up to 9220 bytes. (Regardless of the mode configured on a given jumbo-enabled port, if the port is operating at only 10 Mbps or 100 Mbps, only packets that do not exceed 1522 bytes are allowed inbound on that port.)

## Terminology

**Jumbo Packet:** An IP packet exceeding 1522 bytes in size. The maximum Jumbo packet size is 9220 bytes. (This size includes 4 bytes for the VLAN tag.)

**Jumbo VLAN:** A VLAN configured to allow inbound jumbo traffic. All ports belonging to a jumbo and operating at 1 Gbps or higher can receive jumbo packets from external devices.

**MTU** (*Maximum Transmission Unit)*: This is the maximum-size IP packet the switch can receive for Layer 2 packets inbound on a port. The switch allows jumbo packets of up to 9220 bytes.

**Standard MTU:** An IP packet of 1522 bytes in size. (This size includes 4 bytes for the VLAN tag.)

## Operating Rules

- **Required Port Speed:** The switches allow inbound and outbound jumbo packets on ports operating at speeds of 1 gigabit or higher. At lower port speeds, only standard (1522-byte or smaller) packets are allowed, regardless of the jumbo configuration.
- **Flow Control:** Disable flow control (the default setting) on any ports or trunks through which you want to transmit or receive jumbo packets. Leaving flow control enabled on a port can cause a high rate of jumbo drops to occur on the port.
- **GVRP Operation:** A VLAN enabled for jumbo traffic cannot be used to create a dynamic VLAN. A port belonging to a statically configured, jumbo-enabled VLAN cannot join a dynamic VLAN.
- **Port Adds and Moves:** If you add a port to a VLAN that is already configured for jumbo traffic, the switch enables that port to receive jumbo traffic. If you remove a port from a jumbo-enabled VLAN, the switch disables jumbo traffic capability on the port only if the port is not currently a member of another jumbo-enabled VLAN. This same operation applies to port trunks.
- **Jumbo Traffic Sources:** A port belonging to a jumbo-enabled VLAN can receive inbound jumbo packets through any VLAN to which it belongs, including non-jumbo VLANs. For example, if VLAN 10 (without jumbos enabled) and VLAN 20 (with jumbos enabled) are both configured on a switch, and port 1 belongs to both VLANs, then port 1 can receive jumbo

traffic from devices on either VLAN. For a method to allow only some ports in a VLAN to receive jumbo traffic, refer to "Operating Notes for Jumbo Traffic-Handling" on page 2-25.

## Configuring Jumbo Packet Operation

| Command | Page |
|---|---|
| show vlans | 2-24 |
| show vlans ports < port-list > | 2-24 |
| show vlans < vid > | 2-25 |
| jumbo | 2-25 |

### Overview

1. Determine the VLAN membership of the ports or trunks through which you want the switch to accept inbound jumbo traffic. For operation with GVRP enabled, refer to the GVRP topic under "Operating Rules" , above.
2. Ensure that the ports through which you want the switch to receive jumbo packets are operating at least at gigabit speed. (Check the **Mode** field in the output for the **show interfaces brief *< port-list >*** command.)
3. Use the **jumbo** command to enable jumbo packets on one or more VLANs statically configured in the switch. (All ports belonging to a jumbo-enabled VLAN can receive jumbo packets.
4. Execute **write memory** to save your configuration changes to the startup-config file.

### Viewing the Current Jumbo Configuration

***Syntax:*** show vlans

*Lists the static VLANs configured on the switch and includes a* **Jumbo** *column to indicate which VLANs are configured to support inbound jumbo traffic. All ports belonging to a jumbo-enabled VLAN can receive jumbo traffic. (For more information refer to "Operating Notes for Jumbo Traffic-Handling" on page 2-25.) See figure 2-1, below.*

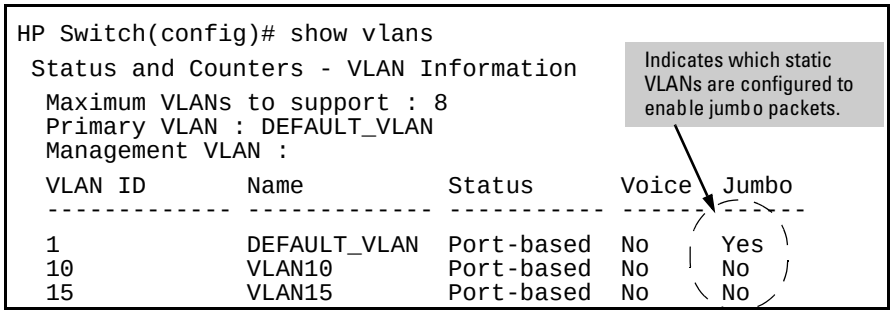



**Figure 2-1. Example Listing of Static VLANs To Show Jumbo Status Per VLAN**

***Syntax:*** show vlans ports < *port-list* > [detailed]

*Lists the static VLANs to which the specified port(s) belong, including the* **Jumbo** *column to indicate which VLANs are configured to support jumbo traffic. Entering only one port in < port-list > results in a list of all VLANs to which that port belongs. Entering multiple ports in < port-list > results in a superset list that includes the VLAN memberships of all ports in the list, even though the individual ports in the list may belong to different subsets of the complete VLAN listing. For example, if port 1 belongs to VLAN 1, port 2 belongs to VLAN 10, and port 3 belongs to VLAN 15, then executing this command with a < port-list > of* **1-3** *results in a listing of all three VLANs, even though none of the ports belong to all three VLANS. (Refer to figure 2-2.)*

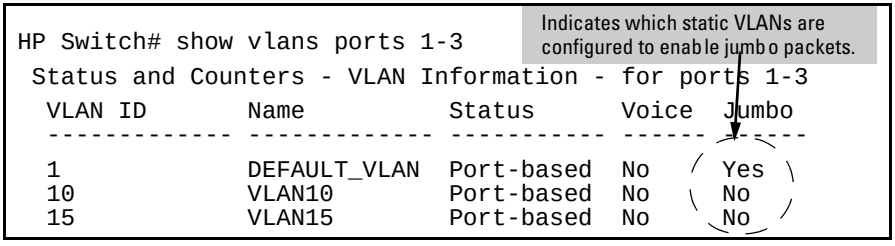



**Figure 2-2. Example of Listing the VLAN Memberships for a Range of Ports**

***Syntax:*** show vlans < *vid* >

*This command shows port membership and jumbo configuration for the specified < vid >.*

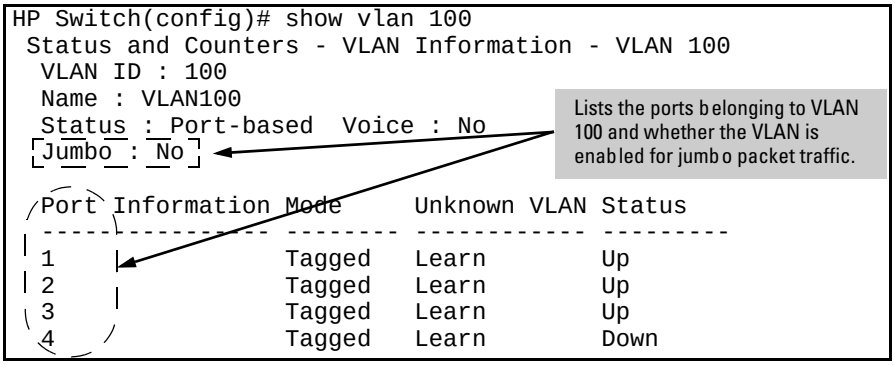



**Figure 2-3. Example of Listing the Port Membership and Jumbo Status for a VLAN**

## Enabling or Disabling Jumbo Traffic on a VLAN

***Syntax:*** vlan < *vid* > jumbo
[ no ] vlan < *vid* > jumbo

*Configures the specified VLAN to allow jumbo packets on all ports on the switch that belong to that VLAN. If the VLAN is not already configured on the switch,* **vlan *< vid >* jumbo** *also creates the VLAN. Note that a port belonging to one jumbo VLAN can receive jumbo packets through any other VLAN statically configured on the switch, regardless of whether the other VLAN is enabled for jumbo packets. The* **[no]** *form of the command disables inbound jumbo traffic on all ports in the specified VLAN that do not also belong to another VLAN that is enabled for jumbo traffic. In a VLAN context, the command forms are* **jumbo** *and* **no jumbo**. *(Default: Jumbos disabled on the specified VLAN.)*

# Operating Notes for Jumbo Traffic-Handling

- HP does not recommend configuring a voice VLAN to accept jumbo packets. Voice VLAN packets are typically small, and allowing a voice VLAN to accept jumbo packet traffic can degrade the voice transmission performance.
- You can configure the default, primary, and/or (if configured) the management VLAN to accept jumbo packets on all ports belonging to the VLAN.
- When the switch applies the default MTU (1522-bytes) to a VLAN, all ports in the VLAN can receive incoming packets of up to 1522 bytes in length. When the switch applies the jumbo MTU (9220 bytes) to a VLAN, all ports in that VLAN can receive incoming packets of up to 9220 bytes in length.

A port receiving packets exceeding the applicable MTU drops such packets, causing the switch to generate an Event Log message and increment the "Giant Rx" counter (displayed by **show interfaces < *port-list* >**).

- The switch does not allow flow control and jumbo packet capability to co-exist on a port. Attempting to configure both on the same port generates an error message in the CLI and sends a similar message to the Event Log.
- The default MTU is 1522 bytes (including 4 bytes for the VLAN tag). The jumbo MTU is 9220 bytes (including 4 bytes for the VLAN tag).
- When a port is not a member of any jumbo-enabled VLAN, it drops all jumbo traffic. If the port is receiving "excessive" inbound jumbo traffic, the port generates an Event Log message to notify you of this condition. This same condition generates a Fault-Finder message in the Alert log of the switch's Web browser interface, and also increments the switch's "Giant Rx" counter.
- If you do not want all ports in a given VLAN to accept jumbo packets, you can consider creating one or more jumbo VLANs with a membership comprised of only the ports you want to receive jumbo traffic. Because a port belonging to one jumbo-enabled VLAN can receive jumbo packets through any VLAN to which it belongs, this method enables you to include both jumbo-enabled and non-jumbo ports within the same VLAN. For example, suppose you wanted to allow inbound jumbo packets only on ports 6, 7, 12, and 13. However, these ports are spread across VLAN 100 and VLAN 200, and also share these VLANs with other ports you want excluded from jumbo traffic. A solution is to create a third VLAN with the sole purpose of enabling jumbo traffic on the desired ports, while leaving the other ports on the switch disabled for jumbo traffic.

  That is:

| | VLAN 100 | VLAN 200 | VLAN 300 |
|---|---|---|---|
| **Ports** | 6-10 | 11-15 | 6, 7, 12, and 13 |
| **Jumbo- Enabled?** | No | No | Yes |

  If there are security concerns with grouping the ports as shown for VLAN 300, you can either use source-port filtering to block unwanted traffic paths or create separate jumbo VLANs, one for ports 6 and 7, and another for ports 12 and 13.
- **Outbound Jumbo Traffic.** Any port operating at 1 Gbps or higher can transmit outbound jumbo packets through any VLAN, regardless of the jumbo configuration. The VLAN is not required to be jumbo-enabled, and the port is not required to belong to any other, jumbo enabled VLANs. This can occur in situations where a non-jumbo VLAN includes some ports that

do not belong to another, jumbo-enabled VLAN and some ports that do belong to another, jumbo-enabled VLAN. In this case, ports capable of receiving jumbo packets can forward them to the ports in the VLAN that do not have jumbo capability.

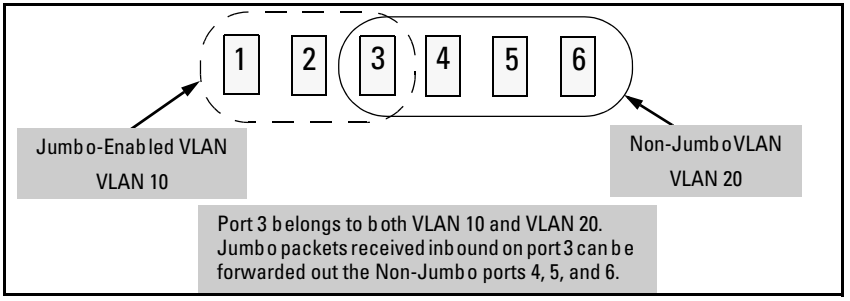



**Figure 2-4. Forwarding Jumbo Packets Through Non-Jumbo Ports**

Jumbo packets can also be forwarded out non-jumbo ports when the jumbo packets received inbound on a jumbo-enabled VLAN are routed to another, non-jumbo VLAN for outbound transmission on ports that have no memberships in other, jumbo-capable VLANs. Where either of the above scenarios is a possibility, the downstream device must be configured to accept the jumbo traffic. Otherwise, this traffic will be dropped by the downstream device.

## Troubleshooting

**A VLAN is configured to allow jumbo packets, but one or more ports drops all inbound jumbo packets.** The port may not be operating at 1 gigabit or higher. Regardless of a port's configuration, if it is actually operating at a speed lower than 1 gigabit, it drops inbound jumbo packets. For example, if a port is configured for **Auto** mode (**speed-duplex auto**), but has negotiated a 100 Mbps speed with the device at the other end of the link, then the port cannot receive inbound jumbo packets. To determine the actual operating speed of one or more ports, view the **Mode** field in the output for the following command:

show interfaces brief < *port-list* >

**A non-jumbo port is generating "Excessive undersize/giant packets" messages in the Event Log.** The switch can transmit outbound jumbo traffic on any port, regardless of whether the port belongs to a jumbo VLAN. In this case, another port in the same VLAN on the switch may be jumbo-enabled through membership in a different, jumbo-enabled VLAN, and may be forwarding jumbo packets received on the jumbo VLAN to non-jumbo ports. Refer to "Outbound Jumbo Traffic" on page 2-26.

# Using Friendly (Optional) Port Names

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Configure Friendly Port Names | Standard Port Numbering | n/a | page 29 | n/a |
| Display Friendly Port Names | n/a | n/a | page 30 | n/a |

This feature enables you to assign alphanumeric port names of your choosing to augment automatically assigned numeric port names. This means you can configure meaningful port names to make it easier to identify the source of information listed by some **Show** commands. (Note that this feature *augments* port numbering, but *does not replace* it.)

## Configuring and Operating Rules for Friendly Port Names

- At either the global or context configuration level you can assign a unique name to a port. You can also assign the same name to multiple ports.
- The friendly port names you configure appear in the output of the **show name [** ***port-list*** **]**, **show config**, and **show interface <** ***port-number*** **>** commands. They do not appear in the output of other show commands or in Menu interface screens. (Refer to "Displaying Friendly Port Names with Other Port Data" on page 2-30.)
- Friendly port names are not a substitute for port numbers in CLI commands or Menu displays.
- Trunking ports together does not affect friendly naming for the individual ports. (If you want the same name for all ports in a trunk, you must individually assign the name to each port.)
- A friendly port name can have up to 64 contiguous alphanumeric characters.
- Blank spaces within friendly port names are not allowed, and if used, cause an **invalid input** error. (The switch interprets a blank space as a name terminator.)
- In a port listing, a blank entry indicates that the port does not have a name assignment other than its fixed port number.

- To retain friendly port names across reboots, you must save the current running-configuration to the startup-config file after entering the friendly port names. (In the CLI, use the **write memory** command.)

## Configuring Friendly Port Names

***Syntax:*** interface < *port-list* > name < *port-name-string* >
*Assigns a port name to port-list.*

***Syntax:*** no interface < *port-list* > name
*Deletes the port name from port-list.*

**Configuring a Single Port Name.** Suppose that you have connected port 9 on the switch to Bill Smith's workstation, and want to assign Bill's name and workstation IP address (10.25.101.73) as a port name for port 9:

```
HP Switch(config)# int 9 name
Bi1l_Smith@10.25.101.73
HP Switch(config)# write mem
HP Switch(config)# show name 9
 Port Names
  Port : 9
   Type : 10/100TX
```

**Figure 2-16. Example of Configuring a Friendly Port Name**

**Configuring the Same Name for Multiple Ports.** Suppose that you want to use ports 11 through 13 as a trunked link to a server used by a drafting group. In this case you might configure ports 11 through 13 with the name "Draft-Server:Trunk".

```
HP Switch(config)# int 11-13 name Draft-Server:Trunk
HP Switch(config)# write mem
HP Switch(config)# show name 11-13

 Port Names

  Port : 11
   Type : 100/1000T
   Name : Draft-Server:Trunk

  Port : 12
   Type : 100/1000T
   Name : Draft-Server:Trunk

  Port : 13
   Type : 100/1000T
   Name : Draft-Server:Trunk
```

**Figure 2-17. Example of Configuring One Friendly Port Name on Multiple Ports**

## Displaying Friendly Port Names with Other Port Data

You can display friendly port name data in the following combinations:

- **show name**: Displays a listing of port numbers with their corresponding friendly port names and also quickly shows you which ports do not have friendly name assignments. (**show name** data comes from the running-config file.)
- **show interface <*port-number*>**: Displays the friendly port name, if any, along with the traffic statistics for that port. (The friendly port name data comes from the running-config file.)
- **show config**: Includes friendly port names in the per-port data of the resulting configuration listing. (**show config** data comes from the startup-config file.)

**To List All Ports or Selected Ports with Their Friendly Port Names.**

This command lists names assigned to a specific port.

***Syntax:*** show name [ *port-list* ]

*Lists the friendly port name with its corresponding port number and port type. The* **show name** *command without a port list shows this data for all ports on the switch.*

For example:

```
HP Switch(config)# show name

 Port Names

  Port Type      Name
  ---- --------- ------------------------------
  1    100/1000T
  2    100/1000T
  3    100/1000T
  4    100/1000T
  5    100/1000T
  6    100/1000T Print_Server
  7    100/1000T Herbert_PC
  8    100/1000T
  9    100/1000T
  10   100/1000T Bill_Smith@10.25.101.73
  11   100/1000T Draft-Server:Trunk
  12   100/1000T Draft-Server:Trunk
  13   100/1000T Draft-Server:Trunk
```

Ports Without "Friendly"

Friendly port names assigned in previous examples.

**Figure 2-18. Example of Friendly Port Name Data for All Ports on the Switch**

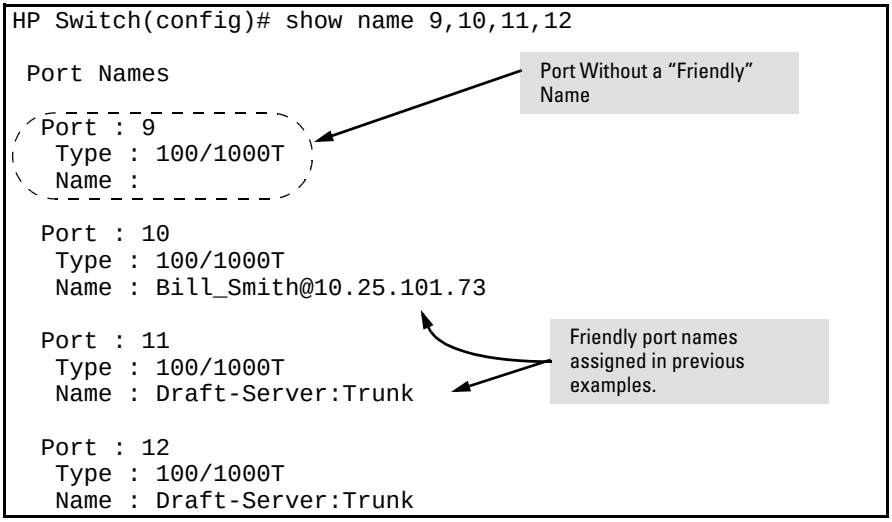



**Figure 2-19. Example of Friendly Port Name Data for Specific Ports on the Switch**

**Including Friendly Port Names in Per-Port Statistics Listings.** A friendly port name configured to a port is automatically included when you display the port's statistics output.

***Syntax:*** show interface < *port-number* >

*Includes the friendly port name with the port's traffic statistics listing.*

For example, if you configure port 5 with the name "O'Connor_10.25.101.43", the show interface output for this port appears similar to the following:

```
HP Switch(config)# show int 5

 Status and Counters - Port Counters for port 5

  Name   : O'Connor@10.25.101.43 <-- Friendly Port Name

  Name   :
  MAC Address      : 001ffe-74b3fb
  Link Status      : Down
  Totals (Since boot or last clear) :
   Bytes Rx        : 0                  Bytes Tx        : 0
   Unicast Rx      : 0                  Unicast Tx      : 0
   Bcast/Mcast Rx  : 0                  Bcast/Mcast Tx  : 0
  Errors (Since boot or last clear) :
   FCS Rx          : 0                  Drops Rx        : 0
   Alignment Rx    : 0                  Collisions Tx   : 0
   Runs Rx         : 0                  Late Colln Tx   : 0
   Giants Rx       : 0                  Excessive Colln : 0
   Total Rx Errors : 0                  Deferred Tx     : 0
  Others (Since boot or last clear) :
   Discard Rx      : 0                  Out Queue Len   : 0
   Unknown Protos  : 0
  Rates (5 minute weighted average) :
   Total Rx  (bps) : 0                  Total Tx  (bps) : 0
   Unicast Rx (Pkts/sec) : 0            Unicast Tx (Pkts/sec) : 0
   B/Mcast Rx (Pkts/sec) : 0            B/Mcast Tx (Pkts/sec) : 0
   Utilization Rx  :     0 %            Utilization Tx  :     0 %
```

**Figure 2-20. Example of a Friendly Port Name in a Per-Port Statistics Listing**

For a given port, if a friendly port name does not exist in the running-config file, the `Name` line in the above command output appears blank:

```
Name   :
```

**To Search the Configuration for Ports with Friendly Port Names.**

This option tells you which friendly port names have been saved to the startup-config file. (**show config** does not include ports that have only default settings in the startup-config file.)

***Syntax:*** show config

*Includes friendly port names in a listing of all interfaces (ports) configured with non-default settings. Excludes ports that have neither a friendly port name nor any other non-default configuration settings.*

For example, if you configure port 6 with a friendly port name:

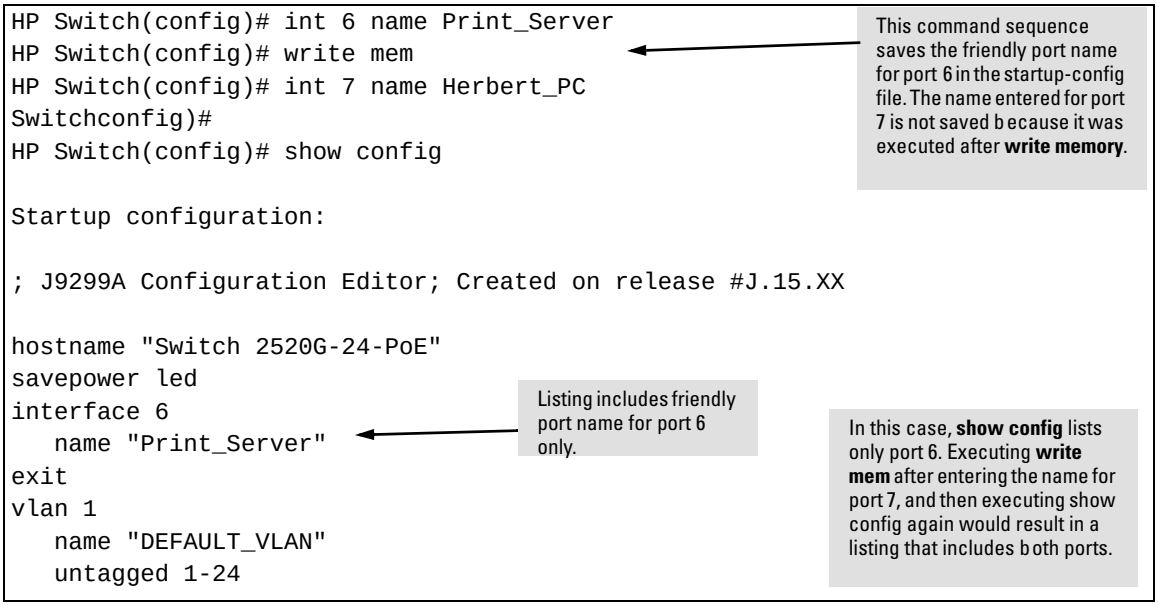



**Figure 2-21. Example Listing of the Startup-Config File with a Friendly Port Name Configured (and Saved)**

## Configuring Transceivers That Haven't Been Inserted

### Transceivers

Previously, a port had to be valid and verified for the switch to allow it to be configured. Transceivers are removable ports and considered invalid when not present in the switch, so they cannot be configured unless they are already in the switch. For switches covered in this guide, the verification for allowable port configurations performed by the CLI is removed and configuration of transceivers is allowed even if they are not yet inserted in the switch.

# Uni-Directional Link Detection (UDLD)

Uni-directional Link Detection (UDLD) monitors a link between two HP Networking switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks. Figure 2-22 shows an example.

**Scenario 1 (No UDLD)**: Without UDLD, the switch ports remain enabled despite the link failure. Traffic continues to be load-balanced to the ports connected to the failed link.

**Scenario 2 (UDLD-enabled)**: When UDLD is enabled, the feature blocks the ports connected to the failed link.

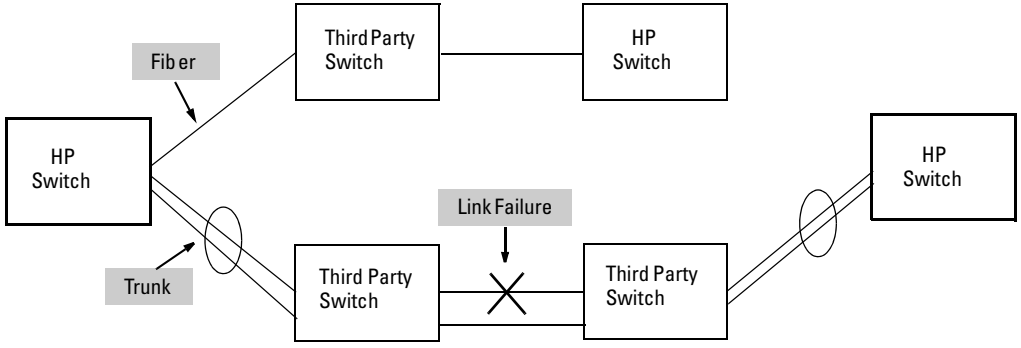



**Figure 2-22. UDLD Example**

In this example, each HP switch load balances traffic across two ports in a trunk group. Without the UDLD feature, a link failure on a link that is not directly attached to one of the HP switches remains undetected. As a result, each switch continue to send traffic on the ports connected to the failed link. When UDLD is enabled on the trunk ports on each HP switch, the switches detect the failed link, block the ports connected to the failed link, and use the remaining ports in the trunk group to forward the traffic.

Similarly, UDLD is effective for monitoring fiber optic links that use two uni-direction fibers to transmit and receive packets. Without UDLD, if a fiber breaks in one direction, a fiber port may assume the link is still good (because the other direction is operating normally) and continue to send traffic on the

connected ports. UDLD-enabled ports; however, will prevent traffic from being sent across a bad link by blocking the ports in the event that either the individual transmitter or receiver for that connection fails.

Ports enabled for UDLD exchange health-check packets once every five seconds (the link-keepalive interval). If a port does not receive a health-check packet from the port at the other end of the link within the keepalive interval, the port waits for four more intervals. If the port still does not receive a health-check packet after waiting for five intervals, the port concludes that the link has failed and blocks the UDLD-enabled port.

When a port is blocked by UDLD, the event is recorded in the switch log or via an SNMP trap (if configured); and other port blocking protocols, like spanning tree or meshing, will not use the bad link to load balance packets. The port will remain blocked until the link is unplugged, disabled, or fixed. The port can also be unblocked by disabling UDLD on the port.

## Configuring UDLD

When configuring UDLD, keep the following considerations in mind:

- UDLD is configured on a per-port basis and must be enabled at both ends of the link. See the note below for a list of HP switches that support UDLD.
- To configure UDLD on a trunk group, you must configure the feature on each port of the group individually. Configuring UDLD on a trunk group's primary port enables the feature on that port only.
- Dynamic trunking is not supported. If you want to configure a trunk group that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the trunk group, you can re-add the UDLD configuration.

**Note**

UDLD interoperates with the following HP switches: 2600, 2800, 3400, 3500, 4200, 5300, 5400, 6200, 6400, 6600, 8212, and 9300. Consult the release notes and current manuals for required software versions.

The following commands allow you to configure UDLD via the CLI.

***Syntax:*** [no] interface <*port-list*> link-keepalive

*Enables UDLD on a port or range of ports.*
*To disable the feature, enter the* **no** *form of the command.*
*Default: UDLD disabled*

***Syntax:*** link-keepalive interval <*interval*>

*Determines the time interval to send UDLD control packets. The <interval> parameter specifies how often the ports send a UDLD packet. You can specify from 10 – 100, in 100 ms increments, where 10 is 1 second, 11 is 1.1 seconds, and so on.*
*Default: 50 (5 seconds)*

***Syntax:*** link-keepalive retries <*num*>

*Determines the maximum number of retries to send UDLD control packets. The <num> parameter specifies the maximum number of times the port will try the health check. You can specify a value from 3 – 10.*
*Default: 5*

***Syntax:*** [no] interface <*port-list*> link-keepalive vlan <*vid*>

*Assigns a VLAN ID to a UDLD-enabled port for sending of tagged UDLD control packets.Under default settings, untagged UDLD packets can still be transmitted and received on tagged only ports—however, a warning message will be logged.*
*The* **no** *form of the command disables UDLD on the specified port(s).*
*Default: UDLD packets are untagged; tagged only ports will transmit and receive untagged UDLD control packets*

## Enabling UDLD

UDLD is enabled on a per port basis. For example, to enable UDLD on port a1, enter:

```
HP Switch(config)#interface al link-keepalive
```

To enable the feature on a trunk group, enter the appropriate port range. For example:

```
HP Switch(config)#interface al-a4 link-keepalive
```

**Note**

When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLD-configured ports in the same vlan. That is, UDLD control packets will “pass through” a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

## Changing the Keepalive Interval

By default, ports enabled for UDLD send a link health-check packet once every 5 seconds. You can change the interval to a value from 10 – 100 deciseconds, where 10 is 1 second, 11 is 1.1 seconds, and so on. For example, to change the packet interval to seven seconds, enter the following command at the global configuration level:

```
HP Switch(config)# link-keepalive interval 70
```

## Changing the Keepalive Retries

By default, a port waits five seconds to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries four more times by sending up to four more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

You can change the maximum number of keepalive attempts to a value from 3 – 10. For example, to change the maximum number of attempts to 4, enter the following command at the global configuration level:

```
HP Switch(config)# link-keepalive retries 4
```

## Configuring UDLD for Tagged Ports

The default implementation of UDLD sends the UDLD control packets untagged, even across tagged ports. If an untagged UDLD packet is received by a non-HP switch, that switch may reject the packet. To avoid such an occurrence, you can configure ports to send out UDLD control packets that are tagged with a specified VLAN.

To enable ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter a command such as the following at the interface configuration level:

```
HP Switch(config)#interface l link-keepalive vlan 22
```

**Notes**

- You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.
- If a VLAN ID is not specified, then UDLD control packets are sent out of the port as untagged packets.

- To re-assign a VLAN ID, re-enter the command with the new VLAN ID number. The new command will overwrite the previous command setting.
- When configuring UDLD for tagged ports, you may receive a warning message if there are any inconsistencies with the port's VLAN configuration (see page 39 for potential problems).

## Viewing UDLD Information

The following show commands allow you to display UDLD configuration and status via the CLI.

***Syntax:*** show link-keepalive

*Displays all the ports that are enabled for link-keepalive.*

***Syntax:*** show link-keepalive statistics

*Displays detailed statistics for the UDLD-enabled ports on the switch.*

***Syntax:*** clear link-keepalive statistics

*Clears UDLD statistics. This command clears the packets sent, packets received, and transitions counters in the show link-keepalive statistics display.*

To display summary information on all UDLD-enabled ports, enter the **show link-keepalive** command. For example:

```
HP Switch(config)# show link-keepalive

Total link-keepalive enabled ports: 4
Keepalive Retries:  3         Keepalive Interval: 1 sec

Port  Enabled  Physical  Keepalive   Adjacent       UDLD
               Status    Status      Switch         VLAN
-------------------------------------------------------------------
 1    Yes      up        up          00d9d-f9b700     200
 2    Yes      up        up          01560-7b1600
 3    Yes      down      off-line
 4    Yes      up        failure
 5     No      down      off-line
```

Port 1 is UDLD-enabled, and tagged for a specific VLAN.

Port 3 is UDLD-enabled, but has no physical connection.

Port 4 is connected, but is blocked due to a link-keepalive failure

Port 5 has been disabled by the System Administrator.

**Figure 2-23. Example of Show Link-Keepalive Command**

To display detailed UDLD information for specific ports, enter the **show link-keepalive statistics** command. For example:

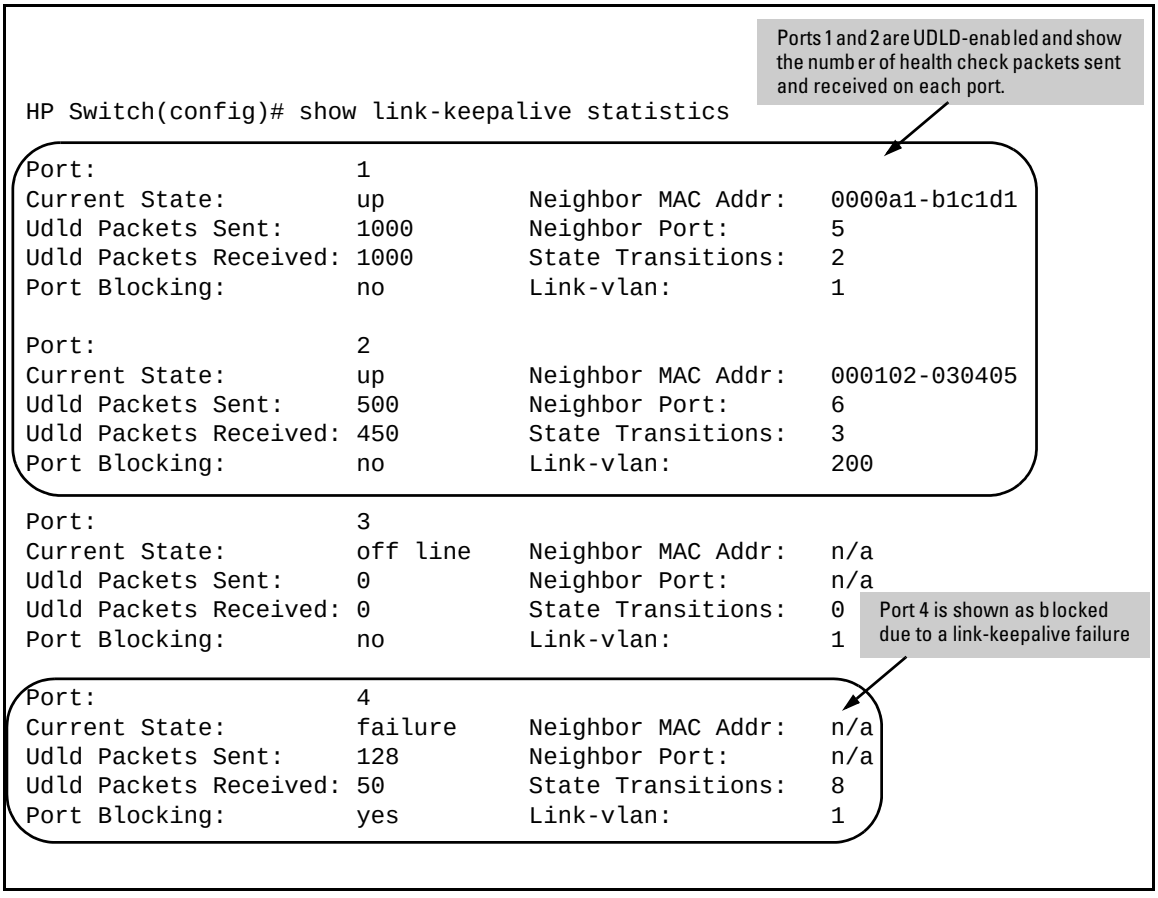



**Figure 2-24. Example of Show Link-Keepalive Statistics Command**

To clear UDLD statistics, enter the following command:

```
HP Switch# clear link-keepalive statistics
```

This command clears the packets sent, packets received, and transitions counters in the **show link keepalive statistics** display (see Figure 2-24 for an example).

## Configuration Warnings and Event Log Messages

Please see the *Event Log Message Reference Guide* for information about Event Log messages.

# Power Over Ethernet (PoE/PoE+) Operation

Power Over Ethernet (PoE/PoE+) technology allows IP telephones, wireless LAN access points, and other powered devices (PDs) to receive power and transfer data over existing LAN cabling.

The switches provision their 10/100Base-TX ports or 10/100/1000Base-TX ports with power for PoE applications compatible with the IEEE 802.3af standard. The PoE ports on your switch support both standard networking links and PoE links. Thus, you can connect either a non-PoE device or a powered device (PD) to a PoE-enabled port without reconfiguring the port.

Table 3-1 shows the power available to the PoE+ ports for the HP 2530 Series switches.

**Table 3-1. PoE+ Power Available for the HP 2530 Series Switches**

| HP Switch | Power Available |
|---|---|
| 8-port 2530 switches | 67 w |
| 24-port 2530 switches | 195 w |
| 48-port 2530 switches | 382 w |

## Configuration Options

In the default configuration, all 10/100Base-TX ports on the HP 2530 switches and 10/100/1000Base-TX ports on the 2530G switches support PoE operation. Using the commands described in this chapter, you can:

- Configure a power threshold for SNMP and Event Log reporting of PoE consumption on the switch.
- Configure per-port priority for allocating power in case the switch becomes oversubscribed and must drop power for some lower-priority ports to support the demand on other, higher-priority ports.
- Disable or re-enable per-port PoE operation on some ports to help control power usage and avoid oversubscribing PoE on the switch.
- Monitor PoE status and performance on the switch.

See “Configuring PoE Operation” on page 3-4 for further details.

## Related Publications

This chapter introduces general PoE operation, PoE configuration and monitoring commands, and event log messages related to PoE operation. The following two manuals provide further information:

- For information on installation, refer to the *HP Series 2530 Switches Installation and Reference Guide*, which is available from the HP website at **www.hp.com/Networking/support**.
- To help you plan and implement a PoE system in your network, refer to the *PoE Planning and Implementation Guide*, which is available from the HP website at **www.hp.com/Networking/support**.

## Terminology

The following PoE terms and concepts are used in this manual.

| Term | Use in this Manual |
|---|---|
| active PoE port | A PoE-enabled port connected to a PD requesting power. |
| priority class | Refers to the type of power prioritization where the switch uses Low (the default), High, and Critical priority assignments to determine which groups of ports will receive power. Note that power priority rules apply only if PoE provisioning on the switch becomes oversubscribed. |
| EPS | External Power Supply. An EPS device provides power to provision PoE ports on a switch. See also "RPS" below. |
| Oversubscribed | The state where there are more PDs requesting PoE power than can be accommodated. |
| MPS | Maintenance Power Signature; the signal a PD sends to the switch to indicate that the PD is connected and requires power. Refer to Figure 3-8 on page 22. |
| PD | Powered Device. A device that receives power through a direct connection to a 10/100 Base-TX PoE RJ-45 port on the switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras. |
| PoE | Power-Over-Ethernet; the method by which PDs receive power from a PoE port (operates according to the IEEE 802.3af standard). Some pre-standard PoE devices are also supported; refer to the FAQs for your switch model. |
| port-number priority | Refers to the type of power prioritization where, within a priority class, the switch assigns the highest priority to the lowest-numbered port, the second-highest priority to the second lowest-numbered port, and so-on. Note that power priority rules apply only if PoE provisioning on the switch becomes oversubscribed. |
| priority class | Refers to the type of power prioritization that uses **Low** (the default), **High**, and **Critical** priority assignments to determine which groups of ports will receive power. Note that power priority rules apply only if PoE provisioning becomes oversubscribed. |

| Term | Use in this Manual |
|---|---|
| PSE | Power-Sourcing Equipment. A PSE provides power to IEEE 802.3af-compliant or IEEE 802.3at-compliant PDs directly connected to the ports. |
| RPS | Redundant Power Supply. An RPS device provides power to a switch if the switch's internal power supply fails. RPS power does not provision PoE ports on a switch whose internal power supply has failed. See also "EPS" above. |

# PoE Operation

## Powered Device (PD) Support

The switch must have a minimum of 17 watts of unused PoE power available when you connect an 802.3af-compliant PD, regardless of how much power the PD actually uses.

Note that once a PD connects to a port and begins operating, the port retains only enough PoE power to support the PD's operation. Unneeded power becomes available for supporting other PD connections. Thus, while 17 watts must be available for the switch to begin supplying power to a port with a PD connected, 17 watts per port is not continually required if the connected PD requires less power.

For example, with 20 watts of PoE power remaining available on the switch, you can connect one new PD without losing power to any currently connected PDs. If that PD draws only 3 watts, then 17 watts remain available and you can connect at least one more PD without interrupting power to any other devices. If the next PD you connect draws 5 watts, then only 12 watts remain unused. With only 12 watts available, if you connect yet another PD, the lowest-priority port will lose PoE power until the switch once again has 17 or more watts available. (For information on power priority, refer to "Power Priority Operation" on page 3-4.)

Disconnecting a PD from a port causes the switch to stop providing PoE power to that port and makes the power available to other ports configured for PoE operation. If the PoE demand becomes greater than the available power, the switch transfers power from lower-priority ports to higher-priority ports. (Ports not currently providing power to PDs are not affected.)

**Note** Depending on power demands, lower-priority ports on a switch with high PoE power demand may occasionally lose power due to the demands of higher-priority ports. (Refer to "Power Priority Operation" for further details.)

## Power Priority Operation

In the default configuration PoE power priority is determined by port number, with the lowest numbered port having the highest priority.

### When Is Power Allocation Prioritized?

If a PSE can provide power for all connected PD demand, it does not use its power priority settings to allocate power. However, if the PD power demand oversubscribes the available power, then the power allocation is prioritized to the ports that present a PD power demand. This causes the loss of power from one or more lower-priority ports to meet the power demand on other, higher-priority ports. This operation occurs regardless of the order in which PDs connect to the switch's PoE-enabled ports.

### How Is Power Allocation Prioritized?

There are two ways that PoE power is prioritized:

- Using a *priority class* method, a power priority of **Low** (the default), **High**, or **Critical** is assigned to each enabled PoE port.
- Using a *port-number priority* method, a lower-numbered port has priority over a higher-numbered port within the same configured priority class, for example, port 1 has priority over port 5 if both are configured with **High** priority.

# Configuring PoE Operation

In the default configuration, PoE support is enabled on the PoE ports. The default priority for all ports is **Low** and the default power notification threshold is **80** (%).

Using the CLI, you can:

- Disable or re-enable PoE operation on individual PoE ports
- Enable support for pre-standard devices

- Change the PoE priority level on individual PoE ports
- Change the threshold for generating a power level notice
- Manually allocate the amount of PoE power for a port by usage, value, or class
- Allocate PoE power based on the link-partner's capabilities via LLDP

## Disabling or Re-Enabling PoE Port Operation

***Syntax:*** [no] interface <*port-list*> power-over-ethernet

Re-enables PoE operation on <port-list > and restores the priority setting in effect when PoE was disabled on <port-list >. The no form of the command disables PoE operation on <port-list >. (Default: All PoE ports are initially enabled for PoE operation at **Low** priority. If you configure a higher priority, this priority is retained until you change it.)

**Note**: For PoE, disabling all ports allows the 22 W of minimum PoE power to be recovered and used elsewhere. You must disable ALL ports for this to occur.

## Enabling Support for Pre-Standard Devices

By default, all HP PoE switches support 802.3af-standard PDs. In addition, the switches covered in this guide have the ability to supply power to pre-802.3af-standard devices, such as legacy (non-standard) IP phones.

**Note**

When the switch is in legacy detection mode, the detection signature range is expanded beyond the IEEE specification. This allows non-compliant devices to be powered.

For a current listing of PDs supported by this feature, visit the HP website at www.hp.com/Networking/support. and select your switch model.

PoE for pre-802.3af-standard powered devices is disabled by default.

***Syntax:*** [no] power pre-std-detect

*The above command enables PoE for pre-802.3af-standard powered devices. The* **no** *form of the command sequence disables PoE for pre-802.3af-standard powered devices. (Default: Disabled)*

To enable this feature, you would enter:

```
HP Switch(config)# power pre-std-detect
```

PoE for pre-802.3af-standard powered devices can be enabled or disabled only from the switch's CLI. This feature cannot be enabled or disabled through either the switch's menu or web browser interfaces.

Executing the **show power-over-ethernet** command lists the system power status as follows:

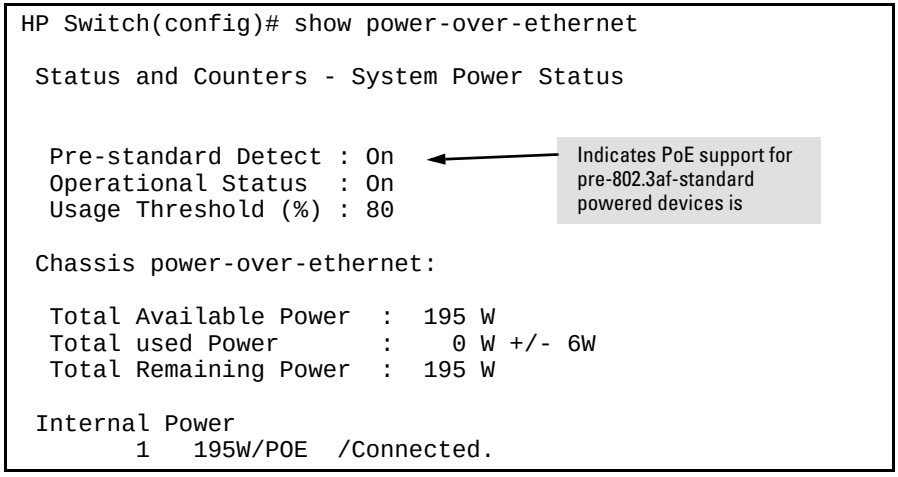



**Figure 3-1. PoE Support for Pre-802.3af-standard Powered Devices Enabled**

For information on the meaning of other power status parameters, refer to “Viewing PoE Configuration and Status” on page 3-18.

# Configuring the PoE Port Priority Level

***Syntax:*** interface < *port-list* > **power-over-ethernet** [ critical | high | low ]

Reconfigures the PoE priority level on <*port-list*>. For a given level, ports are prioritized by port number in ascending order. For example, if ports 1-24 have a priority level of critical, port 1 has priority over ports 2-24.

If there is not enough power available to provision all active PoE ports at a given priority level, then the lowest-numbered port at that level will be provisioned first. PoE priorities are invoked only when all active PoE ports cannot be provisioned (supplied with PoE power).

- **Critical:** Specifies the highest-priority PoE support for <*port-list*>. The active PoE ports at this level are provisioned before the PoE ports at any other level are provisioned.
- **High**: Specifies the second priority PoE support for <*port-list*>. The active PoE ports at this level are provisioned before the Low priority PoE ports are provisioned.
- **Low:** (the default): Specifies the third priority PoE support for <*port-list*>. The active PoE ports at this level are provisioned only if there is power available after provisioning any active PoE ports at the higher priority levels.

Table 3-2 provides examples of how PoE priority settings impact operation.

**Table 3-2. Example of PoE Priority Operation**

| Priority Setting | Configuration Command and Resulting Operation |
|---|---|
| Critical | This priority class always receives power. If there is not enough power to provision PDs on all of the ports configured for this class, then no power goes to ports configured for High and Low priority. If there is enough power to provision PDs on only some of the "Critical" ports, then power is allocated to the "Critical" ports in ascending order, beginning with the lowest-numbered port in the class. For this example, the CLI command to set ports to "Critical" is:<br>`HP Switch(config)# interface 1-3 power critical` |
| High | This priority class receives power only if all PDs on ports with a Critical priority setting are receiving full power. If there is not enough power to provision PDs on all ports with a High priority, then no power goes to ports with a Low priority. If there is enough power to provision PDs on only some of the "High" ports, then power is allocated to the "High" ports in ascending order until all available power is in use. For this example, the CLI command to set ports to "High" is:<br>`HP Switch(config)# interface 4-7 power high` |

| Priority Setting | Configuration Command and Resulting Operation |
|---|---|
| Low | This priority class receives power only if all PDs on ports with High and Critical priority settings are receiving power. If there is enough power to provision PDs on only some Low priority ports, then power is allocated to the ports in ascending order, beginning with the lowest-numbered port in the class until all available power is in use. For this example, the CLI command to set ports to "Low" is:<br>`HP Switch(config)# interface 8-14 power low` |
| - n/a - | For this example, PoE is disabled on these ports. The CLI command for this setting is:<br>`HP Switch(config)# no interface 15-23 power` |

## Controlling PoE Allocation

The default option for PoE allocation is **usage**, which is what a PD attached to the port is allocated. You can override this value by specifying the amount of power allocated to a port by using the **class** or **value** options.

***Syntax:***[no] int <port-list> poe-allocate-by [usage | class | value]

Allows you to manually allocate the amount of PoE power for a port by either its class or a defined value.

**usage**: The automatic allocation by a PD

**class:** Uses the power ramp-up signature of the PD to identify which power class the device will be in. Classes and their ranges are shown in table 3-3.

**value:** A user-defined level of PoE power allocated for that port.

**Note**

The allowable PD requirements are lower than those specified for PSEs to allow for power losses along the Cat-5 cable.

**Table 3-3. Power Classes and Their Values**

| Power Class | Value |
|---|---|
| 0 | Depends on cable type and PoE architecture. Maximum power level output of 15.4 watts at the PSE.<br>This is the default class; if there isn't enough information about the load for a specific classification, the PSE classifies the load as class 0 (zero). |
| 1 | Requires at least 4 watts at the PSE. |
| 2 | Requires at least 7 watts at the PSE. |

| Power Class | Value |
|---|---|
| 3 | 15.4 watts |
| 4 | For PoE+<br>Maximum power level output of 30 watts at the PSE. |

For example, to allocate by class for ports 6 - 8:

```
HP Switch(config)# int 6-8 PoE-allocate-by class
```

## Manually Configuring PoE Power Levels

You can specify a power level (in watts) allocated for a port by using the **value** option. This is the maximum amount of power that will be delivered.

To configure a port by value, first set the PoE allocation by entering the **poe-allocate-by value** command:

```
HP Switch(config)# int 6 poe-allocate-by value
```

or in interface context:

```
HP Switch(eth-6)# poe-allocate-by value
```

Then select a value:

```
HP Switch(config)# int 6 poe-value 15
```

or in interface context:

```
HP Switch(eth-6)# poe-value 15
```

To view the settings, enter the **show power-over-ethernet** command:

```
HP Switch(config)# show power-over-ethernet 6

 Status and Counters - Port Power Status for port 6

  Power Enable      : Yes
                                      LLDP Detect       : enabled
  Priority          : low             Configured Type   :
  AllocateBy        : value           Value             : 15 W
  Power Class       : 2               Detection  Status : Deliverin

  Over Current Cnt  : 0               MPS Absent Cnt    : 0
  Power Denied Cnt  : 0               Short Cnt         : 0

  Voltage           : 49.1 V          Current           : 154 mA
  Power             : 8.4 W
```

Maximum power delivered

**Figure 3-1. Example Displaying PoE Allocation by Value and the Maximum Power Delivered**

If you set the PoE maximum value to less than the PD requires, a fault occurs.

```
HP Switch(config)# interface 7 poe-value 4

HP Switch(config)# show power-over-ethernet 7

 Status and Counters - Port Power Status for port 7

  Power Enable      : Yes
                                      LLDP Detect       : enabled
  Priority          : low             Configured Type   :
  AllocateBy        : value           Value             : 4 W
  Power Class       : 2               Detection  Status : Other Fault

  Over Current Cnt  : 0               MPS Absent Cnt    : 0
  Power Denied Cnt  : 2               Short Cnt         : 0

  Voltage           : 49.1 V          Current           : 154 mA
  Power             : 8.4 W
```

**Figure 3-2. Example Showing PoE Power Value Set Too Low for the PD**

## Changing the Threshold for Generating a Power Notice

By default, PoE support is enabled on the switch's 10/100Base-TX ports, with the power priority set to **Low** and the power threshold set to **80** (%). The following commands allow you to adjust these settings.

***Syntax:*** power threshold < 1 - 99 >

The power threshold is a configurable percentage of the total PoE power available on the switch. When PoE consumption exceeds the threshold, the switch automatically generates an SNMP trap and also sends a message to the Event Log. For example, if the power threshold is set to 80% (the default), and an increasing PoE power demand crosses this threshold, the switch sends an SNMP trap and generates this Event Log message:

```
PoE usage has exceeded threshold of 80 %.
```

If the switch is configured for debug logging, it also sends the same message to the configured debug destination(s).

The switch automatically invokes the power threshold at the global configuration level with a default setting of 80%. You can configure the power threshold to a value in the range of 1% to 99%.

If an increasing PoE power load (1) exceeds the configured power threshold (which triggers the log message and SNMP trap), and then (2) later begins decreasing and drops below the threshold again, the switch generates another SNMP trap, plus a message to the Event Log and any configured Debug destinations. To continue the above example:

```
PoE usage is below configured threshold of 80 %.
```

(Refer to “PoE Event Log Messages” on page 3-23.)

## Cycling Power on a Port

Simply disabling a PoE port does *not* affect power delivery through that port. To cycle the power on a PD receiving power from a PoE port on the switch, disable, then re-enable the power to that port.

***Syntax:*** [no] interface [e] < *port-list* > power

Re-enables PoE operation on < port-list > and restores the priority setting in effect when PoE was disabled on < port-list >. The [no] form of the command disables PoE operation on < port-list >. (Default: All 10/100Base-TX ports on the switch enabled for PoE operation at **Low** priority.)

For example, to cycle the power on a PoE device connected to port 1 on a switch covered in this guide:

```
HP Switch(config)# no interface 1 power
HP Switch(config)# interface 1 power
```

# PoE/PoE+ Allocation Using LLDP Information

## LLDP with PoE

When using PoE, enabling **poe-lldp-detect** allows automatic power configuration if the link partner supports PoE. When LLDP is enabled, the information about the power usage of the PD is available and the switch can then comply with or ignore this information. You can configure PoE on each port according to the PD (IP phone, wireless device, etc.) specified in the LLDP field. The default configuration is for PoE information to be ignored if detected through LLDP.

**Note**

Detecting PoE information via LLDP only affects power delivery; it does not affect normal Ethernet connectivity.

To enable or disable ports for allocating power using LLDP, use this command.

***Syntax:*** int <port-list> poe-lldp-detect [enabled | disabled]

Enables or disables port(s) for allocating PoE power based on the link-partner's capabilities via LLDP.
Default: Disabled

For example, you can enter this command to enable LLDP detection:

```
HP Switch(config)# int 7 poe-lldp-detect enabled
```

or in interface context:

```
HP Switch(eth-7)# poe-lldp-detect enabled
```

To enable PoE detection via LLDP TLV advertisement, use this command and insert the desired port or ports:

```
HP Switch(config)# lldp config <port-number>
medTlvenable poe
```

# LLDP with PoE+

## Overview

The data link layer classification (DLC) for PoE provides more exact control over the power requirement between a PSE and PD. The DLC works in conjunction with the physical layer classification (PLC) and is mandatory for any Type-2 PD that requires more than 12.95 watts of input power.

**Note** DLC is defined as part of the IEEE 802.3at standard.

The power negotiation between a PSE and a PD can be implemented at the physical layer or at the data link layer. After the link is powered at the physical layer, the PSE can use LLDP to repeatedly query the PD to discover the power needs of the PD. Communication over the data link layer allows finer control of power allotment, which makes it possible for the PSE to supply dynamically the power levels needed by the PD. Using LLDP is optional for the PSE but mandatory for a Type 2 PD that requires more than 12.95 watts of power.

If the power needed by the PD is not available, that port is shut off.

## PoE Allocation

LLDP can negotiate power with a PD using LLDP MED TLVs. These are disabled by default. but can be enabled using the **int <*port-list*> PoE-lldp-detect [enabled | disabled]** command, as shown below.

Enabling **PoE-lldp-detect** allows the data link layer to be used for power negotiation.When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied is increased. PoE and LLDP interact to meet the current power demands.

***Syntax:*** int <*port-list*> PoE-lldp-detect [enabled | disabled]

*Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP.*
*Default: Disabled*

For example, you can enter this command to enable LLDP detection:

```
HP Switch(config)# int 7 PoE-lldp-detect enabled
```

or in interface context:

```
HP Switch(eth-7)# PoE-lldp-detect enabled
```

**Note**

Detecting PoE information via LLDP only affects power delivery; it does not affect normal Ethernet connectivity.

You can view the settings by entering the **show power-over-ethernet brief** command:

```
HP Switch(config)# show power-over-ethernet brief

Status and Counters - Port Power Status


  PoE    | Power  Power    Alloc Alloc Actual Configured  Detection   Power
  Port   | Enable Priority By    Power Power  Type        Status      Class
  ------ + ------ -------- ----- ----- ------ ----------- ----------- -----
  1      | Yes    low      usage 17 W  5.0 W  Phone1      Delivering  1
  2      | Yes    low      usage 17 W  0.0 W              Searching   0
  3      | Yes    low      usage 17 W  0.0 W              Searching   0
  4      | Yes    low      usage 17 W  0.0 W              Searching   0
  5      | Yes    low      usage 17 W  0.0 W              Searching   0
  6      | Yes    low      usage 17 W  0.0 W              Searching   0
```

**Figure 3-3. Example of Port with LLDP Configuration Information Obtained from the Device**

## Displaying PoE When Using LLDP Information

To display information about LLDP port configuration, use the **show lldp config** command.

***Syntax***: show lldp config <port-list>

*Displays the LLDP port configuration information, including the TLVs advertised.*

```
HP Switch(config)# show lldp config 4

 LLDP Port Configuration Detail

  Port : 4
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config
   * poe_config

    IpAddress Advertised:
```

**Figure 3-4. Example of LLDP Port Configuration Information with PoE**

Figure 3-5 shows an example of the local device power information using the **show lldp info local-device <*port-list*>** command.

```
HP switch(config) show lldp info local-device 1

LLDP Local Port Information Detail

  Port     : 1
  PortType : local
  PortId   : 1
  PortDesc : 1
  Pvid     : 1

Poe Plus Information Detail

    Poe Device Type            : Type2 PSE
    Power Source               : Primary
    Power Priority             : low
    PD Requested Power Value   : 20 Watts
    PSE Actual Power Value     : 20 Watts
```

**Figure 3-5. Example of Local Power Information**

Figure 3-6 shows an example of the remote device power information using the **show lldp info remote-device <*port-list*>** command.

```
HP switch(config) show lldp info remote-device 3

LLDP Remote Device Information Detail

  Local Port   : 3
  ChassisType  : mac-address
  ChassisId    : 00 16 35 ff 2d 40
  PortType     : local
  PortId       : 23
  SysName      : HPSwitch
  System Descr : HP Switch 2530, revision YA.15.xx
  PortDescr    : 23
  Pvid         : 55

  System Capabilities Supported  : bridge, router
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.0.102.198


  Poe Plus Information Detail

    Poe Device Type            : Type2 PD
    Power Source               : Only PSE
    Power Priority             : low
    PD Requested Power Value   : 20 Watts
    PSE Actual Power Value     : 20 Watts
```

**Figure 3-6. Example of Remote Power Information**

## Operating Note

The advertisement of power with TLVs for LLDP PoE+ is enabled by default. If LLDP is disabled at runtime and a PD is using PoE+ power that has been negotiated through LLDP, there will be a temporary power drop. The port will begin using PoE+ power through the PLC. This event is recorded in the event log. An example message would look like the following:

```
W 08/04/10 13:35:50 02768 ports: Port 1 PoE power
dropped. Exceeded physical classification for a PoE
Type1 device (LLDP process disabled)
```

When LLDP is enabled again, it causes a temporary power drop. This event is also recorded in the event log. An example message looks like the following:

```
W 08/04/10 13:36:31 02771 ports: Port 1 PoE power
dropped. Exceeded physical classification due to
change in classification type (LLDP process enabled)
```

# Viewing PoE Configuration and Status

## Displaying the Switch's Global PoE Power Status

***Syntax:*** show power-over-ethernet

Displays the switch's global PoE power status, including:

- **Pre-standard Detect**: Shows whether *PoE for pre-802.3af-standard powered devices* is enabled on the switch. (Default: **Off**; shows **On** *when PoE for pre-802.3af-standard powered devices has been enabled.)*
- **Operational Status:** Indicates whether PoE power is available on the switch. (Default: **On**; shows **Off** if PoE power is not available. Shows **Faulty** if internal or external PoE power is oversubscribed or faulty.)
- **Usage Threshold (%)**: Lists the configured percentage of available PoE power provisioning the switch must exceed to generate a usage notice in the form of an Event Log message and an SNMP trap. If this event is followed by a drop in power provisioning below the threshold, the switch generates another SNMP trap and Event Log message. Event Log messages are also sent to any optionally configured debug destinations. (Default: **80%**)
- **Total Available Power:** Lists the maximum PoE wattage available to provision active PoE ports on the switch. This is the amount of usable power for PDs.
- **Total used Power:** *The power used by the PDs.*
- **Total Remaining Power:** Lists the amount of PoE power still available.

For example, in the default PoE configuration, when the switch is running with several ports supporting PD loads, **show power-over-ethernet** displays data similar to the following:

```
HP Switch(config)# show power-over-ethernet

 Status and Counters - System Power Status


  Pre-standard Detect : On
  Operational Status  : On
  Usage Threshold (%) : 80

 Chassis power-over-ethernet:

  Total Available Power:    67 W
  Total used       Power:    0 W +/- 6W
  Total Remaining Power:    67 W
```

**Figure 3-2. Example of show power-over-ethernet Output**

## Displaying PoE Status on All Ports

***Syntax:*** show power-over-ethernet brief

Displays the following port power status:

- **PoE Port:** Lists all PoE-capable ports on the switch.
- **Power Enable:** Shows **Yes** for ports on which PoE is enabled (the default) and **No** for ports on which PoE is disabled.
- **LLDP Detect**: Shows if LLDP detection is enabled or disabled.
- **Power Priority:** Lists the power priority (**Low**, **High**, and **Critical**) configured on ports enabled for PoE. (For more on this topic, refer to the command description on page 3-7.)
- **Alloc By:** Displays how PoE is allocated (**usage**, **class**, **value**)
- **PoE Val:** The maximum amount of PoE power allocated for that port (expressed in watts). Default: 17W.
- **Configured Type:** Lists the type of PD connected to each port (as configured by the user on the PD device). For example: `Telephone`, `Webcam`, `Wireless`, `Other`.
- **Detection Status:**
  - **Searching:** The port is trying to detect a PD connection.
  - **Delivering:** The port is delivering power to a PD.
  - **Disabled:** *PoE support is disabled on the port. To re-enable, refer to "Configuring PoE Operation" on page 3-4.*
  - **Fault:** *The switch detects a problem with the connected PD.*
- **Power Class:** Shows the 802.3af power class of the PD detected on the indicated port (as configured by the user on the PD device).

For example, **show power-over-ethernet brief** displays this output:

```
HP Switch(config)# show power-over-ethernet brief

 Status and Counters - Port Power Status

  PoE   | Power   LLDP     Power     Alloc PoE  Configured  Detection   Power
  Port  | Enable  Detect   Priority  By    Val  Type        Status      Class
  ----- + ------- -------- --------- ----- ---- ----------- ----------- ------
  1     | Yes     disabled critical  usage 17 W Telephone   Delivering  1
  2     | Yes     disabled critical  usage 17 W Telephone   Delivering  1
  3     | Yes     disabled high      usage 17 W Wireless    Delivering  3
  4     | Yes     disabled high      usage 17 W Wireless    Delivering  3
  5     | Yes     disabled low       usage 17 W             Searching   0
  6     | Yes     disabled low       usage 17 W             Searching   0
  7     | Yes     disabled low       usage 17 W             Searching   0
  8     | Yes     disabled low       usage 17 W             Searching   0
```

**Figure 3-7. Example of show power-over-ethernet brief Output**

## Displaying the PoE Status on Specific Ports

***Syntax:*** show power-over-ethernet <port-list>

Displays the following PoE status and statistics (since the last reboot) for each port in < port-list >:

- **Power Enable:** Shows **Yes** for ports enabled to support PoE (the default) and **No** for ports on which PoE is disabled.
- **Priority:** Lists the power priority (**Low**, **High**, and **Critical**) configured on ports enabled for PoE. (For more on this topic, refer to the power command description under "Configuring PoE Operation" on page 3-4.)
- **Allocate By:** How PoE is allocated (**usage**, **class**, **value**)
- **Detection Status:**
  - **Searching:** The port is available to support a PD connection.
  - **Delivering:** The port is delivering power to a PD.
  - **Disabled:** *PoE support is disabled on the port. To re-enable PoE support, refer to "Configuring PoE Operation" on page 3-4.*
  - **Fault:** *The switch detects a problem with the connected PD.*
- **Over Current Cnt:** Shows the number of times a connected PD has attempted to draw more than 15.4 watts. Each occurrence generates an Event Log message.
- **Power Denied Cnt:** Shows the number of times PDs requesting power on the port have been denied due to insufficient power available. Each occurrence generates an Event Log message.
- **Voltage:** The total voltage, in Volts, being delivered to PDs.
- **Power:** The total power, in Watts, being delivered to PDs.
- **LLDP Detect**: Port is enabled or disabled for allocating PoE power based on the link-partner's capabilities via LLDP
- **Configured Type:** Shows the type of PD detected on the port.
- **Value:** The maximum amount of PoE power allocated for that port (expressed in watts). Default 17W for PoE.
- **Power Class:** Shows the power class of the PD detected on the indicated port.
- **MPS Absent Cnt:** This value shows the number of times a detected PD has no longer requested power from the port. Each occurrence generates an Event Log message. ("MPS" refers to the "Maintenance Power Signature". Refer to "Terminology" on page 3-2.)
- Short Cnt: Shows the number of times the switch provided insufficient current to a connected PD.
- Current: The total current, in mA, being delivered to PDs.

For example, if you wanted to view the PoE status of port 5, you would use **show power-over-ethernet 5** to display the data:

```
HP Switch(config)# show power-over-ethernet 5

 Status and Counters - Port Power Status for port 5

  Power Enable      : Yes
                                      LLDP Detect       : disabled
  Priority          : low             Configured Type   :
  AllocateBy        : usage           Value             : 17 W
  Power Class       : 0               Detection  Status : Searching

  Over Current Cnt  : 0               MPS Absent Cnt    : 0
  Power Denied Cnt  : 0               Short Cnt         : 0

  Voltage           : 0.0 V           Current           : 0 mA
  Power             : 0.0 W
```

**Figure 3-8. Example of Output for show power-over-ethernet for a Port**

# Planning and Implementing a PoE Configuration

This section provides an overview of some considerations for planning a PoE application. For additional information, refer to the HP *PoE Planning and Implementation Guide*.

## Assigning PoE Ports to VLANs

If your network includes VLANs, you may want to assign various PoE-configured ports to specific VLANs. For example, if you are using PoE telephones in your network, you may want to assign ports used for telephone access to a VLAN reserved for telephone traffic.

## Applying Security Features to PoE Configurations

You can utilize security features built into the switch to control device or user access to the network through PoE ports in the same way as non-PoE ports.

- **MAC Address Security:** Using Port Security, you can configure each switch port with a unique list of up to eight MAC addresses for devices that are authorized to access the network through that port. For more information, refer to the chapter titled "Configuring and Monitoring Port Security" in the *Access Security Guide* for your switch.
- **Username/Password Security:** If you are connecting a device that allows you to enter a username and password that is forwarded to a networked server for authentication, then you can also configure the following security features:
  - TACACS+
  - RADIUS Authentication and Accounting
  - 802.1X Authentication

  For more information, refer to the *Access Security Guide* for your switch.

# PoE Event Log Messages

Please see the *Event Log Message Reference Guide* for information about Event Log messages.

# Port Trunking

This chapter describes creating and modifying port trunk groups. This includes non-protocol trunks and LACP (802.3ad) trunks.

**Port Status and Configuration Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port trunks | n/a | page 4-7 | page 4-9 | page 4-14 |
| configuring a static trunk group | none | page 4-7 | page 4-12 | — |
| configuring a dynamic LACP trunk group | disabled | — | page 4-13 | — |

Port trunking allows you to assign up to eight physical links to one logical link (trunk) that functions as a single, higher-speed link providing dramatically increased bandwidth. This capability applies to connections between backbone devices as well as to connections in other network areas where traffic bottlenecks exist. A *trunk group* is a set of up to eight ports configured as members of the same port trunk. Note that the ports in a trunk group do not have to be consecutive. For example:

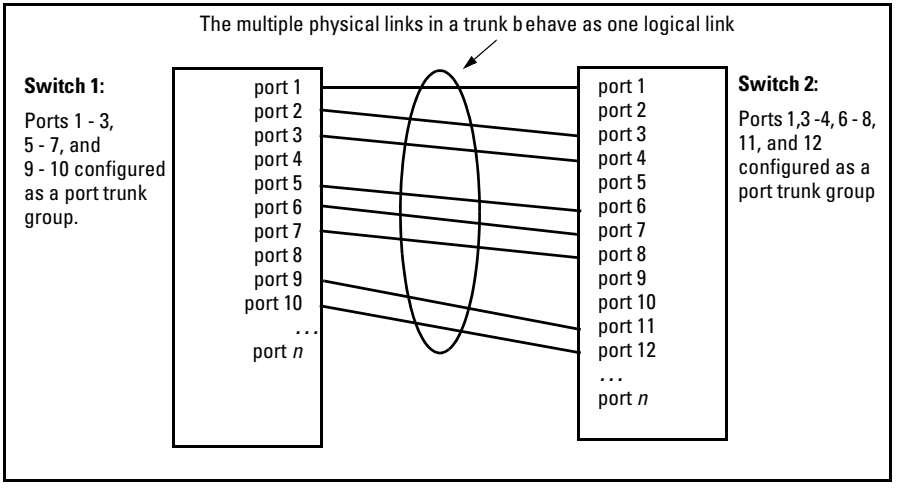



**Figure 4-1. Conceptual Example of Port Trunking**

With full-duplex operation in a eight-port trunk group, trunking enables the following bandwidth capabilities:

**Port Connections and Configuration:** All port trunk links must be point-to-point connections between a switch and another switch, router, server, or workstation configured for port trunking. No intervening, non-trunking devices are allowed. It is important to note that ports on both ends of a port trunk group must have the same mode (speed and duplex) and flow control settings.

**Note**

**Link Connections.** The switch does not support port trunking through an intermediate, non-trunking device such as a hub, or using more than one media type in a port trunk group. Similarly, for proper trunk operation, all links in the same trunk group must have the same speed, duplex, and flow control.

**Port Security Restriction.** Port security does not operate on a trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch resets the port security parameters for those ports to the factory-default configuration.

**Caution**

**To avoid broadcast storms or loops** in your network while configuring a trunk, first disable or disconnect all ports you want to add to or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

# Port Trunk Features and Operation

The switches covered in this guide offer these options for port trunking:

- LACP: IEEE 802.3ad—page 4-15
- Trunk: Non-Protocol—page 4-21

Up to 24 trunk groups are supported on the switches covered in this guide. The actual maximum depends on the number of ports available on the switch and the number of links in each trunk. (Using the Link Aggregation Control Protocol—LACP—option, you can include standby trunked ports in addition to the maximum of eight actively trunking ports.)

**LACP Note**

LACP requires full-duplex (FDx) links of the same media type (10/100Base-T, 100FX, etc.) and the same speed, and enforces speed and duplex conformance across a trunk group. For most installations, HP recommends that you leave the port Mode settings at **Auto** (the default). LACP also operates with **Auto-10**,

**Auto-100**, and **Auto-1000** (if negotiation selects FDx), and **10FDx**, **100FDx**, and **1000FDx** settings. (The 10-gigabit ports available for some switch models allow only the **Auto** setting.)

**Fault Tolerance:** If a link in a port trunk fails, the switch redistributes traffic originally destined for that link to the remaining links in the trunk. The trunk remains operable as long as there is at least one link in operation. If a link is restored, that link is automatically included in the traffic distribution again. The LACP option also offers a standby link capability, which enables you to keep links in reserve for service if one or more of the original active links fails. Refer to "Trunk Group Operation Using LACP" on page 4-15.)

# Trunk Configuration Methods

**Dynamic LACP Trunk**: The switch automatically negotiates trunked links between LACP-configured ports on separate devices, and offers one dynamic trunk option: LACP. To configure the switch to initiate a dynamic LACP trunk with another device, use the **interface** command in the CLI to set the default LACP option to **Active** on the ports you want to use for the trunk. For example, the following command sets ports 1-4 to LACP active:

```
HP Switch(config) int 1-4 lacp active
```

Note that the preceding example works if the ports are not already operating in a trunk. To change the LACP option on ports already operating as a trunk, you must first remove them from the trunk. For example, if ports 1 - 4 were LACP-active and operating in a trunk with another device, you would do the following to change them to LACP-passive:

```
HP Switch(config)# no int 1-4 lacp
```

*Removes the ports from the trunk.*

```
HP Switch(config)# int 1-4 lacp passive
```

*Configures LACP passive.*

**Static Trunk:** The switch uses the links you configure with the Port/Trunk Settings screen in the menu interface or the **trunk** command in the CLI to create a static port trunk. The switch offers two types of static trunks: LACP and Trunk.

**Table 4-1. Trunk Types Used in Static and Dynamic Trunk Groups**

| Trunking Method | LACP | Trunk |
|---|---|---|
| Dynamic | Yes | No |
| Static | Yes | Yes |

**Table 4-2. Trunk Configuration Protocols**

| Protocol | Trunking Options |
|---|---|
| LACP (802.3ad) | Provides dynamic and static LACP trunking options.<br>• **Dynamic LACP** — Use the switch-negotiated dynamic LACP trunk when:<br>– The port on the other end of the trunk link is configured for Active or Passive LACP.<br>– You want fault-tolerance for high-availability applications. If you use an eight-link trunk you can also configure one or more additional links to operate as standby links that will activate only if another active link goes down.<br>• **Static LACP** — Use the manually configured static LACP trunk when:<br>– The port on the other end of the trunk link is configured for a static LACP trunk<br>– You want to configure non-default spanning tree or IGMP parameters on an LACP trunk group.<br>– *You want an LACP trunk group to operate in a VLAN other than the default VLAN and GVRP is disabled. (Refer to "VLANs and Dynamic LACP" on page 4-19.)*<br>– You want to use a monitor port on the switch to monitor an LACP trunk.<br><br>For more information, refer to "Trunk Group Operation Using LACP" on page 4-15. |
| Trunk (non-protocol) | Provides manually configured, static-only trunking to:<br>• Most HP switches not running the 802.3ad LACP protocol.<br>• Windows NT and HP-UX workstations and servers<br>Use the Trunk option when:<br>– The device to which you want to create a trunk link is using a non-802.3ad trunking protocol<br>– You are unsure which type of trunk to use, or the device to which you want to create a trunk link is using an unknown trunking protocol.<br>– You want to use a monitor port on the switch to monitor traffic on a trunk.<br><br>Refer to "Trunk Group Operation Using the "Trunk" Option" on page 4-21. |

**Table 4-3. General Operating Rules for Port Trunks**

**Media:** For proper trunk operation, all ports on both ends of a trunk group must have the same media type and mode (speed and duplex). (For the switches covered in this guide, HP recommends leaving the port Mode setting at **Auto** or, in networks using Cat 3 cabling, **Auto-10**.)

**Port Configuration:** The default port configuration is **Auto**, which enables a port to sense speed and negotiate duplex with an Auto-Enabled port on another device. HP recommends that you use the **Auto** setting for all ports you plan to use for trunking. Otherwise, you must manually ensure that the mode setting for each port in a trunk is compatible with the other ports in the trunk.

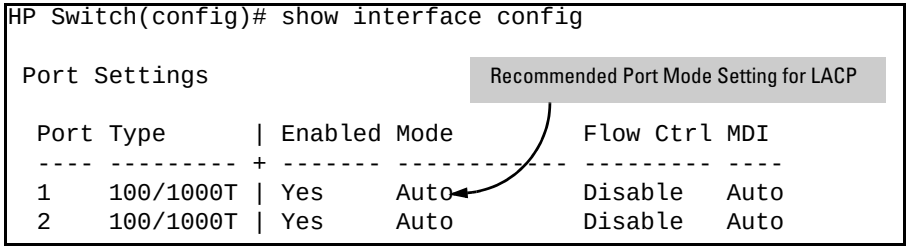



**Figure 4-2. Recommended Port Mode Setting for LACP**

All of the following operate on a per-port basis, regardless of trunk membership:

- Enable/Disable
- Flow control (Flow Ctrl)

LACP is a full-duplex protocol. Refer to "Trunk Group Operation Using LACP" on page 4-15.

**Trunk Configuration:** All ports in the same trunk group must be the same trunk type (LACP or Trunk). All LACP ports in the same trunk group must be either all static LACP or all dynamic LACP.

A trunk appears as a single port labeled **Dyn1** (for an LACP dynamic trunk) or **Trk1** (for a static trunk of type: LACP, Trunk) on various menu and CLI screens. For a listing of which screens show which trunk types, refer to "How the Switch Lists Trunk Data" on page 4-22.

For spanning-tree or VLAN operation, configuration for all ports in a trunk is done at the trunk level. (You cannot separately configure individual ports within a trunk for spanning-tree or VLAN operation.)

**Traffic Distribution:** All of the switch trunk protocols use the SA/DA (Source Address/Destination Address) method of distributing traffic across the trunked links. Refer to "Outbound Traffic Distribution Across Trunked Links" on page 4-22.

**Spanning Tree:** 802.1D (STP) and 802.1w (RSTP) Spanning Tree operate as a global setting on the switch (with one instance of Spanning Tree per switch). 802.1s (MSTP) Spanning Tree operates on a per-instance basis (with multiple instances allowed per switch). For each SpanningTree instance, you can adjust Spanning Tree parameters on a per-port basis. A static trunk of any type appears in the Spanning Tree configuration display, and you can configure Spanning Tree parameters for a static trunk in the same way that you would configure Spanning Tree parameters on a non-trunked port. (Note that the switch lists the trunk by name—such as **Trk1**—and does not list the individual ports in the trunk.) For example, if ports 1 and 2 are configured as a static trunk named **Trk1**, they are listed in the Spanning Tree display as **Trk1** and do not appear as individual ports in the Spanning Tree displays.

In this example showing part of the **show spanning-tree** listing, ports 1 and 2 are members of TRK1 and do not appear as individual ports in the port configuration part of the listing.

```
Port    Type       Cost  Priority State      | Designated Bridge
------- ---------- ----- -------- ---------- + -----------------
3       100/1000T  5     128      Forwarding | 0020c1-h27ac0
4       100/1000T  5     128      Forwarding | 0060b0-889e00
5       100/1000T  5     128      Disabled   |
6       100/1000T  5     128      Disabled   |
Trk1               1     64       Forwarding | 0001e7-a0ec00
```

**Figure 4-3. Example of a Port Trunk in a Spanning Tree Listing**

When Spanning Tree forwards on a trunk, all ports in the trunk will be forwarding. Conversely, when Spanning Tree blocks a trunk, all ports in the trunk are blocked.

**Note:** A dynamic LACP trunk operates only with the default Spanning Tree settings. Also, this type of trunk appears in the CLI **show spanning-tree** display, but not in the Spanning Tree Operation display of the Menu interface.

If you remove a port from a static trunk, the port retains the same Spanning Tree settings that were configured for the trunk.

**IP Multicast Protocol (IGMP):** A static trunk of any type appears in the IGMP configuration display, and you can configure IGMP for a static trunk in the same way that you would configure IGMP on a non-trunked port. (Note that the switch lists the trunk by name—such as **Trk1**—and does not list the individual ports in the trunk.) Also, creating a new trunk automatically places the trunk in IGMP Auto status if IGMP is enabled for the default VLAN. A dynamic LACP trunk operates only with the default IGMP settings and does not appear in the IGMP configuration display or **show ip igmp** listing.

**VLANs:** Creating a new trunk automatically places the trunk in the DEFAULT_VLAN, regardless of whether the ports in the trunk were in another VLAN. Similarly, removing a port from a trunk group automatically places the port in the default VLAN. You can configure a static trunk in the same way that you configure a port for membership in any VLAN.

**Note:** For a dynamic LACP trunk to operate in a VLAN other than the default VLAN (DEFAULT_VLAN), GVRP must be enabled. Refer to "Trunk Group Operation Using LACP" on page 4-15.

**Port Security:** Trunk groups (and their individual ports) cannot be configured for port security, and the switch excludes trunked ports from the **show port-security** listing. If you configure non-default port security settings for a port, then subsequently try to place the port in a trunk, you will see the following message and the command will not be executed:

< *port-list* > `Command cannot operate over a logical port.`

**Monitor Port:**

**Note:** A trunk cannot be a monitor port. A monitor port can monitor a static trunk but cannot monitor a dynamic LACP trunk.

# Menu: Viewing and Configuring a Static Trunk Group

**Important**

Configure port trunking *before* you connect the trunked links to another switch, routing switch, or server. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. Refer to "Enabling or Disabling Ports and Configuring Port Mode" on page 2-14.)

**To View and/or Configure Static Port Trunking:** This procedure uses the Port/Trunk Settings screen to configure a static port trunk group on the switch.

1. Follow the procedures in the Important note above.
2. From the Main Menu, Select:

   **2. Switch Configuration ...**

   **2. Port/Trunk Settings**
3. Press **[E]** (for **Edit**) and then use the arrow keys to access the port trunk parameters.

```
====================- CONSOLE - MANAGER MODE -====================
        Switch Configuration - Port/Trunk Settings

Port    Type       Enabled      Mode       Flow Ctrl  Group  Type
----  --------- + -------  ------------  ---------  -----  -----
1     1000T     | Yes      Auto          Disable
2     1000T     | Yes      Auto          Disable
3     1000T     | Yes      Auto          Disable
4     1000T     | Yes      Auto          Disable
5     1000T     | Yes      Auto          Disable
6     1000T     | Yes      Auto          Disable
```

These two columns indicate static trunk status.

(For dynamic LACP trunk status, use the CLI show lacp command—page 4-10.)

**Figure 4-4. Example of the Menu Screen for Configuring a Port Trunk Group**

4. In the Group column, move the cursor to the port you want to configure.
5. Use the Space bar to choose a trunk group assignment (**Trk1**, **Trk2**, and so on) for the selected port.

- For proper trunk operation, all ports in a trunk must have the same media type and mode (such as 10/100TX set to 100FDx, or 100FX set to 100FDx). The flow control settings must also be the same for all ports in a given trunk. To verify these settings, refer to "Viewing Port Status and Configuring Port Parameters" on page 2-1.
- You can configure the trunk group with up to eight ports per trunk. If multiple VLANs are configured, all ports within a trunk will be assigned to the same VLAN or set of VLANs. (With the 802.1Q VLAN capability built into the switch, more than one VLAN can be assigned to a trunk. Refer to the chapter titled "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.)

  (To return a port to a non-trunk status, keep pressing the Space bar until a blank appears in the highlighted Group value for that port.)

```
==================- CONSOLE - MANAGER MODE -==================
        Switch Configuration - Port/Trunk Settings

Port    Type       Enabled      Mode       Flow Ctrl  Group  Type
----  --------- + -------  ------------  ---------  -----  -----
1     1000T     | Yes      Auto          Disable
2     1000T     | Yes      Auto          Disable
3     1000T     | Yes      Auto          Disable
4     1000T     | Yes      Auto          Disable
5     1000T     | Yes      Auto          Disable    Trk1   Trunk
6     1000T     | Yes      Auto          Disable    Trk1   Trunk
```

**Figure 4-5. Example of the Configuration for a Two-Port Trunk Group**

6. Move the cursor to the Type column for the selected port and use the Space bar to select the trunk type:
   - LACP
   - Trunk (the default type if you do not specify a type)

   All ports in the same trunk group on the same switch must have the same Type (**LACP** or **Trunk)**.

7. When you are finished assigning ports to the trunk group, press **[Enter]**, then **[S]** (for **Save**) and return to the Main Menu. (It is not necessary to reboot the switch.)

   During the Save process, traffic on the ports configured for trunking will be delayed for several seconds. If the Spanning Tree Protocol is enabled, the delay may be up to 30 seconds.

8. Connect the trunked ports on the switch to the corresponding ports on the opposite device. If you previously disabled any of the trunked ports on the switch, enable them now. (Refer to "Viewing Port Status and Configuring Port Parameters" on page 2-1.)

Check the Event Log ("Using the Event Log for Troubleshooting Switch Problems" on page C-17) to verify that the trunked ports are operating properly.

# CLI: Viewing and Configuring Port Trunk Groups

**Trunk Status and Configuration Commands**

| | |
|---|---|
| show trunks | below |
| show lacp | page 4-10 |
| trunk | page 4-12 |
| interface < *port-list* > lacp | page 4-13 |

## Using the CLI To View Port Trunks

You can list the trunk type and group for all ports on the switch or for selected ports. You can also list LACP-only status information for LACP-configured ports.

**Listing Static Trunk Type and Group for All Ports or for Selected Ports.**

***Syntax:*** show trunks [< *port-list* >]

*Omitting the* < port-list > *parameter results in a static trunk data listing for all LAN ports in the switch. For example, in a switch where ports 4 and 5 belong to Trunk 1 and ports 7 and 8 belong to Trunk 2, you have the options shown in figures 4-6 and 4-7 for displaying port data for ports belonging to static trunks.*

Using a port list specifies, for switch ports in a static trunk group, only the ports you want to view. In this case, the command specifies ports 5 through 7. However, because port 6 is not in a static trunk group, it does not appear in the resulting listing:

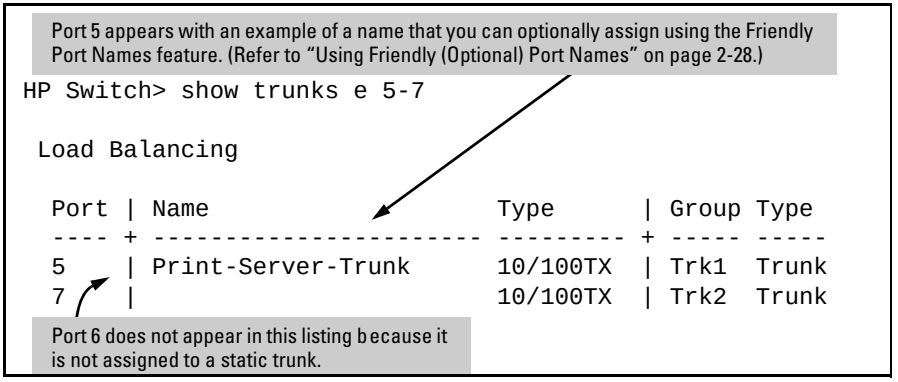



**Figure 4-6. Example Listing Specific Ports Belonging to Static Trunks**

The **show trunks < *port-list* >** command in the above example includes a port list, and thus shows trunk group information only for specific ports that have membership in a static trunk. In figure 4-7, the command does not include a port list, so the switch lists all ports having static trunk membership.

```
HP Switch> show trunks

 Load Balancing

  Port | Name                      Type      | Group Type
  ---- + ------------------------ --------- + ----- -----
  4    | Print-Server-Trunk       10/100TX  | Trk1  Trunk
  5    | Print-Server-Trunk       10/100TX  | Trk1  Trunk
  7    |                          10/100TX  | Trk2  Trunk
  8    |                          10/100TX  | Trk2  Trunk
```

**Figure 4-7. Example of a Show Trunk Listing Without Specifying Ports**

### Listing Static LACP and Dynamic LACP Trunk Data.

***Syntax:*** show lacp

*Lists data for only the LACP-configured ports..*

In the following example, ports 1 and 2 have been previously configured for a static LACP trunk. (For more on the "Active" parameter, see table 4-5 on page 4-17.)

```
HP Switch> show lacp
                                LACP

PORT   LACP      TRUNK     PORT      LACP      LACP
NUMB   ENABLED   GROUP     STATUS    PARTNER   STATUS
----   -------   -------   -------   -------   -------
l      Active    Trkl      Up        Yes       Success
2      Active    Trkl      Up        Yes       Success
3      Active    3         Down      No        Success
4      Passive   4         Down      No        Success
5      Passive   5         Down      No        Success
6      Passive   6         Down      No        Success
```

**Figure 4-8. Example of a Show LACP Listing**

(For a description of each of the above-listed data types, refer to table 4-5, "LACP Port Status Data" on page 4-17.)

**Dynamic LACP Standby Links.** Dynamic LACP trunking enables you to configure standby links for a trunk by including more than eight ports in a dynamic LACP trunk configuration. When eight ports (trunk links) are up, the remaining link(s) will be held in standby status. If a trunked link that is "Up" fails, it will be replaced by a standby link, which maintains your intended bandwidth for the trunk. (Refer to also the "Standby" entry under "Port Status" in "Table 4-5. LACP Port Status Data" on page 4-17.) In the next example, ports 1 through 9 have been configured for the same LACP trunk. Notice that one of the links shows Standby status, while the remaining eight links are "Up".

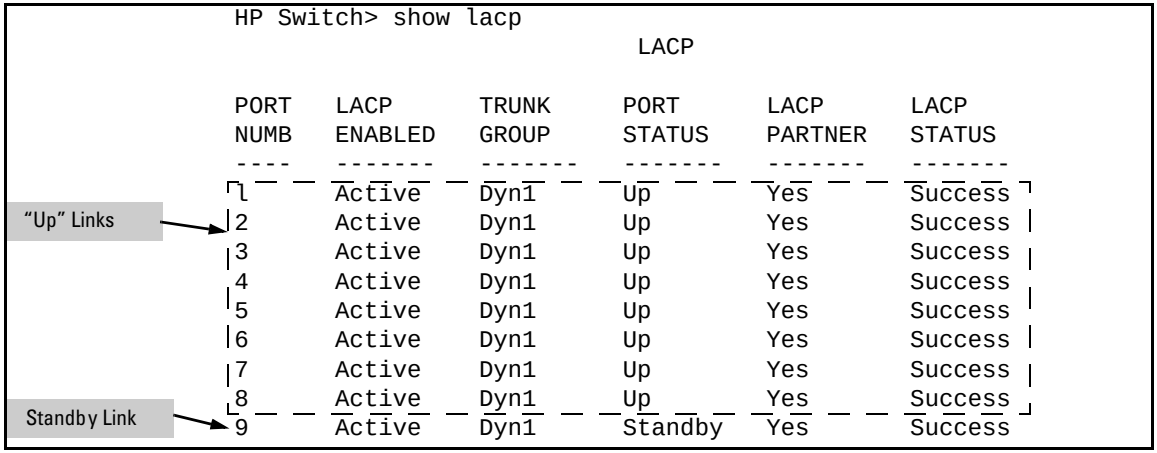



**Figure 4-9. Example of a Dynamic LACP Trunk with One Standby Link**

## Using the CLI To Configure a Static or Dynamic Trunk Group

**Important**

Configure port trunking *before* you connect the trunked links between switches. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. Refer to "Enabling or Disabling Ports and Configuring Port Mode" on page 2-14.)

The table on page 4-4 describes the maximum number of trunk groups you can configure on the switch. An individual trunk can have up to eight links, with additional standby links if you're using LACP. You can configure trunk group types as follows:

| Trunk Type | Trunk Group Membership | |
|---|---|---|
| | Trk*X* (Static) | Dyn*X* (Dynamic) |
| LACP | Yes | Yes |
| Trunk | Yes | No |

The following examples show how to create different types of trunk groups.

**Configuring a Static Trunk or Static LACP Trunk Group.**

***Syntax:*** trunk < *port-list* > < trk1 ... trk24 > < trunk | lacp >

*Configures the specified static trunk type.*

This example uses ports 4 - 6 to create a non-protocol static trunk group with the group name of **Trk2**.

```
HP Switch(config)# trunk 4-6 trk2 trunk
```

**Removing Ports from a Static Trunk Group.** This command removes one or more ports from an existing **Trk*x*** trunk group.

**Caution**

Removing a port from a trunk can create a loop and cause a broadcast storm. When you remove a port from a trunk where spanning tree is not in use, HP recommends that you first disable the port or disconnect the link on that port.

***Syntax:*** no trunk < *port-list* >

*Removes the specified ports from an existing trunk group.*

For example, to remove ports 4 and 5 from an existing trunk group.

```
HP Switch(config)# no trunk 4-5
```

**Enabling a Dynamic LACP Trunk Group.** In the default port configuration, all ports on the switch are set to disabled. To enable the switch to automatically form a trunk group that is dynamic on both ends of the link, the ports on one end of a set of links must be LACP **Active**. The ports on the other end can be either LACP **Active** or LACP **Passive**. The **active** command enables the switch to automatically establish a (dynamic) LACP trunk group when the device on the other end of the link is configured for LACP **Passive**.

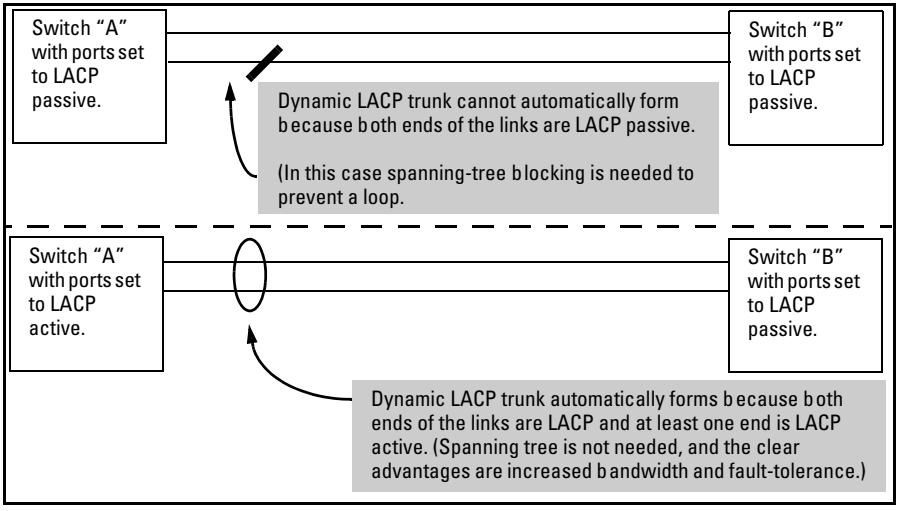



**Figure 4-10. Example of Criteria for Automatically Forming a Dynamic LACP Trunk**

***Syntax:*** interface < *port-list* > lacp active

*Configures < port-list > as LACP active. If the ports at the other end of the links on < port-list > are configured as LACP passive, then this command enables a dynamic LACP trunk group on < port-list >.*

This example uses ports 4 and 5 to enable a dynamic LACP trunk group.

```
HP Switch(config)# interface 4-5 lacp active
```

**Removing Ports from an Dynamic LACP Trunk Group.** To remove a port from dynamic LACP trunk operation, you must turn off LACP on the port. (On a port in an operating, dynamic LACP trunk, you cannot change between LACP **Active** and LACP **passive** without first removing LACP operation from the port.)

**Caution**

Unless spanning tree is running on your network, removing a port from a trunk can result in a loop. To help prevent a broadcast storm when you remove a port from a trunk where spanning tree is not in use, HP recommends that you first disable the port or disconnect the link on that port.

***Syntax:*** no interface < *port-list* > lacp

*Removes < port-list > from any dynamic LACP trunk and returns the ports in < port-list > to passive LACP.*

In this example, port 6 belongs to an operating, dynamic LACP trunk. To remove port 6 from the dynamic trunk and return it to passive LACP, you would do the following:

```
HP Switch(config)# no interface 6 lacp
HP Switch(config)# interface 6 lacp passive
```

Note that in the above example, if the port on the other end of the link is configured for active LACP or static LACP, the trunked link will be re-established almost immediately.

# Web: Viewing Existing Port Trunk Groups

While the web browser interface does not enable you to configure a port trunk group, it does provide a view of an existing trunk group.

To view any port trunk groups:

Click on the **Status** tab.

Click on **[Port Status]**.

# Trunk Group Operation Using LACP

The switch can automatically configure a dynamic LACP trunk group or you can manually configure a static LACP trunk group.

**Note**

LACP requires full-duplex (FDx) links of the same media type (10/100Base-T, 100FX, etc.) and the same speed, and enforces speed and duplex conformance across a trunk group. For most installations, HP recommends that you leave the port Mode settings at **Auto** (the default). LACP also operates with **Auto-10**, **Auto-100**, and **Auto-1000** (if negotiation selects FDx), and **10FDx**, **100FDx**, and **1000FDx** settings.

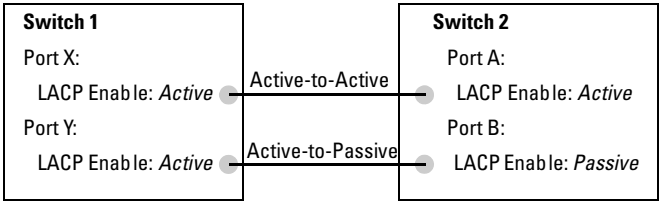
LACP trunk status commands include:

| Trunk Display Method | Static LACP Trunk | Dynamic LACP Trunk |
|---|---|---|
| CLI **show lacp** command | Included in listing. | Included in listing. |
| CLI **show trunk** command | Included in listing. | Not included. |
| Port/Trunk Settings screen in menu interface | Included in listing. | Not included |

Thus, to display a listing of dynamic LACP trunk ports, you must use the **show lacp** command.

In most cases, trunks configured for LACP on the switches covered in this guide operate as described in table 4-4 on the next page.

**Table 4-4. LACP Trunk Types**

| LACP Port Trunk Configuration | Operation |
|---|---|
| Dynamic LACP | This option automatically establishes an 802.3ad-compliant trunk group, with **LACP** for the port Type parameter and **Dyn*X*** for the port Group name, where ***X*** is an automatically assigned value from 1 to 24, depending on how many dynamic and static trunks are currently on the switch. (The switch allows a maximum of 24 trunk groups in any combination of static and dynamic trunks.)<br>**Note:** Dynamic LACP trunks operate only in the default VLAN (unless GVRP is enabled and **Forbid** is used to prevent the trunked ports from joining the default VLAN). Thus, if an LACP dynamic port forms using ports that are not in the default VLAN, the trunk will automatically move to the default VLAN unless GVRP operation is configured to prevent this from occurring. In some cases, this can create a traffic loop in your network. For more on this topic, refer to "VLANs and Dynamic LACP" on page 4-19.<br>Under the following conditions, the switch automatically establishes a dynamic LACP port trunk group and assigns a port Group name:<br>• The ports on both ends of each link have compatible mode settings (speed and duplex).<br>• The port on one end of each link must be configured for LACP Active and the port on the other end of the same link must be configured for either LACP Passive or LACP Active. For example:<br>  <br><br>Either of the above link configurations allow a dynamic LACP trunk link.<br>**Backup Links:** A maximum of eight operating links are allowed in the trunk, but, with dynamic LACP, you can configure one or more additional (backup) links that the switch automatically activates if a primary link fails. To configure a link as a standby for an existing eight-port dynamic LACP trunk, ensure that the ports in the standby link are configured as either active-to-active or active-to-passive between switches.<br>**Displaying Dynamic LACP Trunk Data:** To list the configuration and status for a dynamic LACP trunk, use the CLI **show lacp** command.<br>**Note:** The dynamic trunk is automatically created by the switch, and is not listed in the static trunk listings available in the menu interface or in the CLI **show trunk** listing. |

| LACP Port Trunk Configuration | Operation |
|---|---|
| Static LACP | Provides a manually configured, static LACP trunk to accommodate these conditions:<br>• The port on the other end of the trunk link is configured for a static LACP trunk.<br>• You want to configure non-default spanning tree or IGMP parameters on an LACP trunk group.<br>• You want an LACP trunk group to operate in a VLAN other than the default VLAN and GVRP is disabled. (Refer to "VLANs and Dynamic LACP" on page 4-19.)<br>• You want to use a monitor port on the switch to monitor an LACP trunk.<br>The trunk operates if the trunk group on the opposite device is running one of the following trunking protocols:<br>• Active LACP<br>• Passive LACP<br>• Trunk<br>This option uses **LACP** for the port Type parameter and **Trk*X*** for the port Group parameter, where ***X*** is an automatically assigned value in a range corresponding to the maximum number of trunks the switch allows. (The table on page 4-4 lists the maximum number of trunk groups allowed on the switches covered in this guide.)<br>Displaying Static LACP Trunk Data: To list the configuration and status for a static LACP trunk, use the CLI **show lacp** command. To list a static LACP trunk with its assigned ports, use the CLI **show trunk** command or display the menu interface Port/Trunk Settings screen.<br>Static LACP does not allow standby ports. |

## Default Port Operation

In the default configuration, LACP is disabled for all ports. If LACP is not configured as Active on at least one end of a link, then the port does not try to detect a trunk configuration and operates as a standard, untrunked port. Table 4-5 lists the elements of per-port LACP operation. To display this data for a switch, execute the following command in the CLI:

```
HP Switch> show lacp
```

**Table 4-5. LACP Port Status Data**

| Status Name | Meaning |
|---|---|
| Port Numb | Shows the physical port number for each port configured for LACP operation (1, 2, 3 .)_Unlisted port numbers indicate that the missing ports are assigned to a static Trunk group are not configured for any trunking. |
| LACP Enabled | **Active:** The port automatically sends LACP protocol packets.<br>**Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.<br>A link having either two active LACP ports or one active port and one passive port can perform dynamic LACP trunking. A link having two passive LACP ports will not perform LACP trunking because both ports are waiting for an LACP protocol packet from the opposite device.<br>**Note:** In the default switch configuration, LACP is disabled for all ports. |

| Status Name | Meaning |
|---|---|
| Trunk Group | **Trk*X***: This port has been manually configured into a static LACP trunk.<br>**Trunk Group Same as Port Number:** The port is configured for LACP, but is not a member of a port trunk. |
| Port Status | **Up:** The port has an active LACP link and is not blocked or in Standby mode.<br>**Down:** The port is enabled, but an LACP link is not established. This can indicate, for example, a port that is not connected to the network or a speed mismatch between a pair of linked ports.<br>**Disabled:** The port cannot carry traffic.<br>**Blocked:** LACP, spanning tree has blocked the port. (The port is not in LACP Standby mode.) This may be due to a (brief) trunk negotiation or a configuration error such as differing port speeds on the same link or trying to connect the switch to more trunks than it can support. (See the table on page 4-4.)<br>**Note**: Some older devices are limited to four ports in a trunk. When eight LACP-enabled ports are connected to one of these older devices, four ports connect, but the other four ports are blocked.<br>**Standby:** The port is configured for dynamic LACP trunking to another device, but the maximum number of ports for the Dynamic trunk to that device has already been reached on either the switch or the other device. This port will remain in reserve, or "standby" unless LACP detects that another, active link in the trunk has become disabled, blocked, or down. In this case, LACP automatically assigns a Standby port, if available, to replace the failed port. |
| LACP Partner | **Yes:** LACP is enabled on both ends of the link.<br>**No:** LACP is enabled on the switch, but either LACP is not enabled or the link has not been detected on the opposite device. |
| LACP Status | **Success:** LACP is enabled on the port, detects and synchronizes with a device on the other end of the link, and can move traffic across the link.<br>**Failure:** LACP is enabled on a port and detects a device on the other end of the link, but is not able to synchronize with this device, and therefore not able to send LACP packets across the link. This can be caused, for example, by an intervening device on the link (such as a hub), a bad hardware connection, or if the LACP operation on the opposite device does not comply with the IEEE 802.3ad standard. |

## LACP Notes and Restrictions

**802.1X (Port-Based Access Control) Configured on a Port.** To maintain security, LACP is not allowed on ports configured for 802.1X authenticator operation. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables 802.1X on that port.

```
HP Switch(config)# aaa port-access authenticator 1
LACP has been disabled on 802.1x port(s).
HP Switch(config)#
```

The switch will not allow you to configure LACP on a port on which port access (802.1X) is enabled. For example:

```
HP Switch(config)# int 1 lacp passive
Error configuring port < port-number >: LACP and 802.1x
cannot be run together.
HP Switch(config)#
```

To restore LACP to the port, you must first remove the port's 802.1X configuration and then re-enable LACP active or passive on the port.

**Port Security Configured on a Port.** To maintain security, LACP is not allowed on ports configured for port security. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables port security on that port. For example:

```
HP Switch(config)# port-security 17 learn-mode static
address-limit 2
LACP has been disabled on secured port(s).
HP Switch(config)#
```

The switch will not allow you to configure LACP on a port on which port security is enabled. For example:

```
HP Switch(config)# int 17 lacp passive
Error configuring port 17: LACP and port security cannot
be run together.
```

To restore LACP to the port, you must remove port security and re-enable LACP active or passive.

**Changing Trunking Methods.** To convert a trunk from static to dynamic, you must first eliminate the static trunk.

**Static LACP Trunks.** Where a port is configured for LACP (Active or Passive), but does not belong to an existing trunk group, you can add that port to a static trunk. Doing so disables dynamic LACP on that port, which means you must manually configure both ends of the trunk.

**Dynamic LACP Trunks.** You can configure a port for LACP-active or LACP-passive, but on a dynamic LACP trunk you cannot configure the other options that you can on static trunks. If you want to manually configure a trunk, use the **trunk** command. (Refer to "Using the CLI To Configure a Static or Dynamic Trunk Group" on page 4-12.)

**VLANs and Dynamic LACP.** A dynamic LACP trunk operates only in the default VLAN (unless you have enabled GVRP on the switch and use **Forbid** to prevent the ports from joining the default VLAN).

- If you want to use LACP for a trunk on a non-default VLAN and GVRP is disabled, configure the trunk as a static trunk.

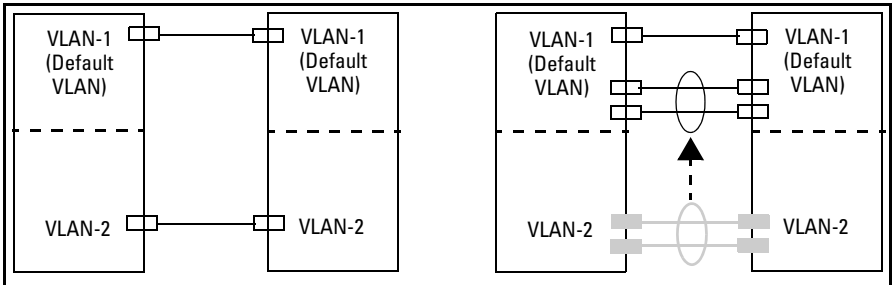
**Blocked Ports with Older Devices.** Some older devices are limited to four ports in a trunk. When eight LACP-enabled ports are connected to one of these older devices, four ports connect, but the other four ports are blocked. The LACP status of the blocked ports is shown as “Failure”.

If one of the other ports becomes disabled, a blocked port will replace it (Port Status becomes “Up”). When the other port becomes active again, the replacement port goes back to blocked (Port Status is “Blocked”). It can take a few seconds for the switch to discover the current status of the ports.

```
HP Switch(eth-1-8)# show lacp
                         LACP
   PORT   LACP      TRUNK     PORT      LACP      LACP
   NUMB   ENABLED   GROUP     STATUS    PARTNER   STATUS
   ----   -------   -------   -------   -------   -------
   1     Active    Dyn1      Up        Yes       Success
   2     Active    Dyn1      Up        Yes       Success
   3     Active    Dyn1      Up        Yes       Success
   4     Active    Dyn1      Up        Yes       Success
   5     Active    Dyn1      Blocked   Yes       Failure
   6     Active    Dyn1      Blocked   Yes       Failure
```

**Figure 4-11. Blocked Ports with LACP**

- If there are ports that you do not want on the default VLAN, ensure that they cannot become dynamic LACP trunk members. Otherwise a traffic loop can unexpectedly occur. For example:




If the ports in VLAN 2 are configured to allow a dynamic trunk (and GVRP is disabled), adding a second link in VLAN 2 automatically forms a dynamic LACP trunk and moves the trunk to VLAN-1 (the default VLAN), which creates a traffic loop in VLAN 1 between the two switches and eliminates the link in VLAN 2 between the two switches.

**Figure 4-12. A Dynamic LACP Trunk Forming in a VLAN Can Cause a Traffic Loop**

Easy control methods include either disabling LACP on the selected ports or configuring them to operate in static LACP trunks.

**Spanning Tree and IGMP.** If Spanning Tree and/or IGMP is enabled in the switch, a dynamic LACP trunk operates only with the default settings for these features and does not appear in the port listings for these features.

**Half-Duplex and/or Different Port Speeds Not Allowed in LACP Trunks.** The ports on both sides of an LACP trunk must be configured for the same speed and for full-duplex (FDx). The 802.3ad LACP standard specifies a full-duplex (FDx) requirement for LACP trunking. (10-gigabit ports operate only at FDx.)

A port configured as LACP passive and not assigned to a port trunk can be configured to half-duplex (HDx). However, in any of the following cases, a port cannot be reconfigured to an HDx setting:

- If the port is a 10-gigabit port.
- If a port is set to LACP Active, you cannot configure it to HDx.
- If a port is already a member of a static or dynamic LACP trunk, you cannot configure it to HDx.
- If a port is already set to HDx, the switch does not allow you to configure it for a static or dynamic LACP trunk.

**Dynamic/Static LACP Interoperation:** A port configured for dynamic LACP can properly interoperate with a port configured for static (Trk*X*) LACP, but any ports configured as standby LACP links will be ignored.

# Trunk Group Operation Using the "Trunk" Option

This method creates a trunk group that operates independently of specific trunking protocols and does not use a protocol exchange with the device on the other end of the trunk. With this choice, the switch simply uses the SA/DA method of distributing outbound traffic across the trunked ports without regard for how that traffic is handled by the device at the other end of the trunked links. Similarly, the switch handles incoming traffic from the trunked links as if it were from a trunked source.

When a trunk group is configured with the **trunk** option, the switch automatically sets the trunk to a priority of "4" for spanning-tree operation (even if spanning-tree is currently disabled. This appears in the running-config file as `spanning-tree Trkn priority 4`. Executing **write memory** after configuring the trunk places the same entry in the startup-config file.

Use the Trunk option to establish a trunk group between a switch covered in this guide and another device, where the other device's trunking operation fails to operate properly with LACP trunking configured on the switches.

# How the Switch Lists Trunk Data

Static Trunk Group: Appears in the menu interface and the output from the CLI **show trunk** and **show interfaces** commands.

Dynamic LACP Trunk Group: Appears in the output from the CLI **show lacp** command.

| Interface Option | Dynamic LACP Trunk Group | Static LACP Trunk Group | Static Non-Protocol |
|---|---|---|---|
| Menu Interface | No | Yes | Yes |
| CLI **show trunk** | No | Yes | Yes |
| CLI **show interfaces** | No | Yes | Yes |
| CLI **show lacp** | Yes | Yes | No |
| CLI **show spanning-tree** | No | Yes | Yes |
| CLI **show igmp** | No | Yes | Yes |
| CLI **show config** | No | Yes | Yes |

# Outbound Traffic Distribution Across Trunked Links

The two trunk group options (LACP and Trunk) use source-destination address pairs (SA/DA) for distributing outbound traffic over trunked links. SA/DA (source address/destination address) causes the switch to distribute outbound traffic to the links within the trunk group on the basis of source/destination address pairs. That is, the switch sends traffic from the same source address to the same destination address through the same trunked link,

and may also send traffic from the same source address to a different destination address through the same link or a different link, depending on the mapping of path assignments among the links in the trunk. Likewise, the switch distributes traffic for the same destination address but from different source addresses through links depending on the path assignment.

The load-balancing is done on a per communication basis. Otherwise, traffic is transmitted across the same path as shown in figure 4-13. That is, if Client A attached to Switch 1 sends five packets of data to Server A attached to Switch 2, the same link is used to send all five packets. The SA/DA address pair for the traffic is the same. The packets are not evenly distributed across any other existing links between the two switches; they all take the same path.

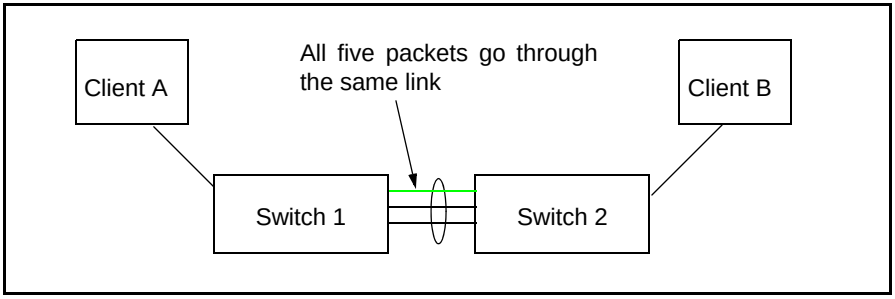



**Figure 4-13. Example of Single Path Traffic through a Trunk**

The actual distribution of the traffic through a trunk depends on a calculation using bits from the Source Address and Destination address. When an IP address is available, the calculation includes the last five bits of the IP source address and IP destination address, otherwise the MAC addresses are used. The result of that process undergoes a mapping that determines which link the traffic goes through. If you have only two ports in a trunk, it is possible that all the traffic will be sent through one port even if the SA/DA pairs are different. The more ports you have in the trunk, the more likely it is that the traffic will be distributed among the links.

When a new port is added to the trunk, the switch begins sending traffic, either new traffic or existing traffic, through the new link. As links are added or deleted, the switch redistributes traffic across the trunk group. For example, in figure 4-14 showing a three-port trunk, traffic could be assigned as shown in table 4-6.

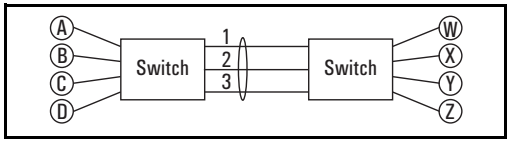



**Figure 4-14. Example of Port-Trunked Network**

**Table 4-6. Example of Link Assignments in a Trunk Group (SA/DA Distribution)**

| Source: | Destination: | Link: |
|---|---|---|
| Node A | Node W | 1 |
| Node B | Node X | 2 |
| Node C | Node Y | 3 |
| Node D | Node Z | 1 |
| Node A | Node Y | 2 |
| Node B | Node W | 3 |

Because the amount of traffic coming from or going to various nodes in a network can vary widely, it is possible for one link in a trunk group to be fully utilized while other links in the same trunk have unused bandwidth capacity even if the assignments were evenly distributed across the links in a trunk.

# Configuring for Network Management Applications

## Using SNMP Tools To Manage the Switch

### Overview

You can manage the switch via SNMP from a network management station running an application such as IMC. For more on IMC, visit the HP web site at: **www.hp.com/Networking** and navigate to Network management.

This section includes:

- An overview of SNMP management for the switch
- Configuring the switches for:
  - SNMP Communities (page 5-9)
  - Trap Receivers and Authentication Traps (page 5-14)
- Information on advanced management through RMON Support (page 5-28)

To implement SNMP management, the switch must have an IP address, configured either manually or dynamically (using DHCP or Bootp). If multiple VLANs are configured, each VLAN interface should have its own IP address. For DHCP use with multiple VLANs, refer to the section titled "The Primary VLAN" in the "Static Virtual LANs (VLANs)" chapter of the *Advanced Traffic Management Guide* for your switch.

**Note**

If you use the switch's Authorized IP Managers and Management VLAN features, ensure that the SNMP management station and/or the choice of switch port used for SNMP access to the switch are compatible with the access controls enforced by these features. Otherwise, SNMP access to the switch will be blocked. For more on Authorized IP Managers, refer to the *Access Security Guide* for your switch. (The latest version of this guide is available on the HP web site.) For information on the Management VLAN feature, refer to the section titled "The Secure Management VLAN" in the "Static Virtual LANs (VLANs)" chapter of the *Advanced Traffic Management Guide* for your switch.

## SNMP Management Features

SNMP management features on the switch include:

- SNMP version 1, version 2c, or version 3 over IP
- Security via configuration of SNMP communities (page 5-9)
- Security via authentication and privacy for SNMP Version 3 access
- Event reporting via SNMP
  - Version 1 traps
  - RMON: groups 1, 2, 3, and 9
- IMC support
- Flow sampling using sFlow
- Standard MIBs, such as the Bridge MIB (RFC 1493), Ethernet MAU MIB (RFC 1515), and others.

The switch SNMP agent also uses certain variables that are included in a Hewlett-Packard proprietary MIB (Management Information Base) file. If you are using HP OpenView, you can ensure that it is using the latest version of the MIB file by downloading the file to the OpenView database. To do so, go to the HP web site at:

**www.hp.com/Networking**

Click on **Support**, and enter your product number

## Configuring for SNMP version 1 and 2c Access to the Switch

SNMP access requires an IP address and subnet mask configured on the switch. (Refer to *Basic Operation Guide*.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (Refer to *Basic Operation Guide*.)

Once an IP address has been configured, the main steps for configuring SNMP version 1 and version 2c access management features are:

1. Configure the appropriate SNMP communities. (Refer to “SNMPv3 Communities” on page 5-9.)
2. Configure the appropriate trap receivers. (Refer to “SNMP Notifications” on page 5-14.)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct community name may access the switch with the View and Access levels that have been set for that community.

If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (Refer to the *Access Security Guide* for your switch.)

**Caution**

For PCM version 1.5 or earlier (or any TopTools version), deleting the "public" community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and you are using the above software versions, HP recommends that you change the write access for the "public" community to "Restricted".

## Configuring for SNMP Version 3 Access to the Switch

SNMP version 3 (SNMPv3) access requires an IP address and subnet mask configured on the switch. (Refer to *Basic Operation Guide*.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See *Basic Operation Guide*.)

Once an IP address has been configured, the main steps for configuring SNMP version 3 access management features are:

1. Enable SNMPv3 for operation on the switch (Refer to "SNMP Version 3 Commands" on page 5-4)
2. Configure the appropriate SNMP users (Refer to "SNMPv3 Users" on page 5-5)
3. Configure the appropriate SNMP communities. (Refer to "SNMPv3 Communities" on page 5-9.)
4. Configure the appropriate trap receivers. (Refer to "SNMP Notifications" on page 5-14.)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct User and community name may access the switch with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (Refer to the *Access Security Guide* for your switch.)

## SNMP Version 3 Commands

SNMP version 3 (SNMPv3) adds some new commands to the CLI for configuring SNMPv3 functions. To enable SMNPv3 operation on the switch, use the **snmpv3 enable** command. An initial user entry will be generated with MD5 authentication and DES privacy.

You may (optionally) restrict access to only SNMPv3 agents by using the **snmpv3 only** command. To restrict write-access to only SNMPv3 agents, use the **snmpv3 restricted-access** command.

**Caution**

Restricting access to only version 3 messages will make the community named "public" inaccessible to network management applications (such as auto-discovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the switch.

***Syntax:*** [no] snmpv3 enable

*Enable and disable the switch for access from SNMPv3 agents. This includes the creation of the initial user record.*

[no] snmpv3 only

*Enables or disables restrictions to access from only SNMPv3 agents. When enabled, the switch will reject all non-SNMPv3 messages.*

[no] snmpv3 restricted-access

*Enables or disables restrictions from all non-SNMPv3 agents to read only access.*

show snmpv3 enable

*Displays the operating status of SNMPv3.*

show snmpv3 only

*Displays status of message reception of non-SNMPv3 messages.*

show snmpv3 restricted-access

*Displays status of write messages of non-SNMPv3 messages.*

## Enabling SNMPv3

The **snmpv3 enable** command allows the switch to:

- Receive SNMPv3 messages.
- Configure initial users.
- Restrict non-version 3 messages to "read only" (optional).

Figure 5-1 shows an example of how to use the **snmpv3 enable** command.

**Note: SNMP Version 3 Initial Users**

To create new users, most SNMPv3 management software requires an initial user record to clone. The initial user record can be downgraded and provided with fewer features, but not upgraded by adding new features. For this reason it is recommended that when you enable SNMPv3, you also create a second user with SHA authentication and DES privacy.

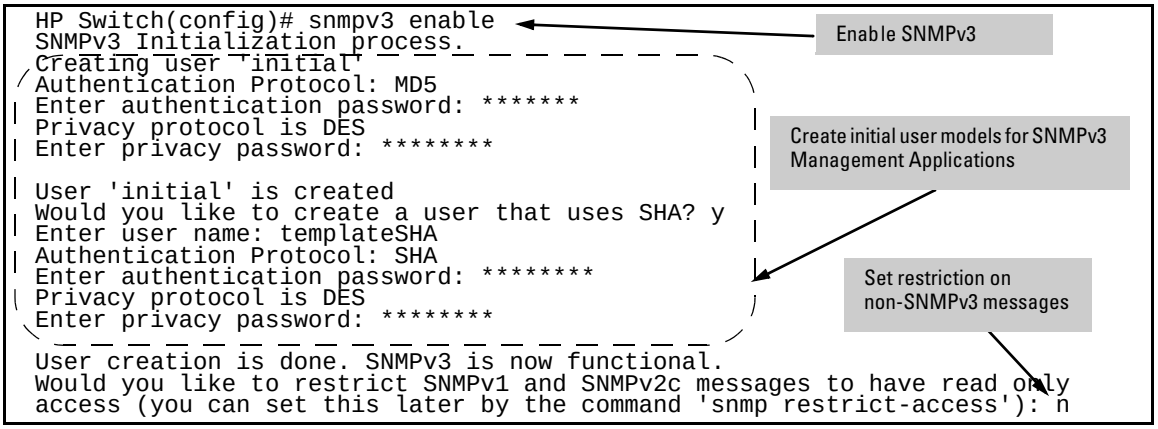



**Figure 5-1. Example of SNMP version 3 Enable Command**

## SNMPv3 Users

To use SNMPv3 on the switch, you must configure the users that will be assigned to different groups. To configure SNMP users on the switch:

1. Configure users in the User Table with the **snmpv3 user** command. To view the list of configured users, enter the **show snmpv3 user** command (see "Adding Users" on page 5-6).
2. Assign users to Security Groups based on their security model with the **snmpv3 group** command (see "Assigning Users to Groups" on page 5-7).

**Caution** If you add an SNMPv3 user without authentication and/or privacy to a group that requires either feature, the user will not be able to access the switch. Ensure that you add a user with the appropriate security level to an existing security group.

**Adding Users.** To configure an SNMPv3 user, you must first add the user name to the list of known users with the **snmpv3 user** command.

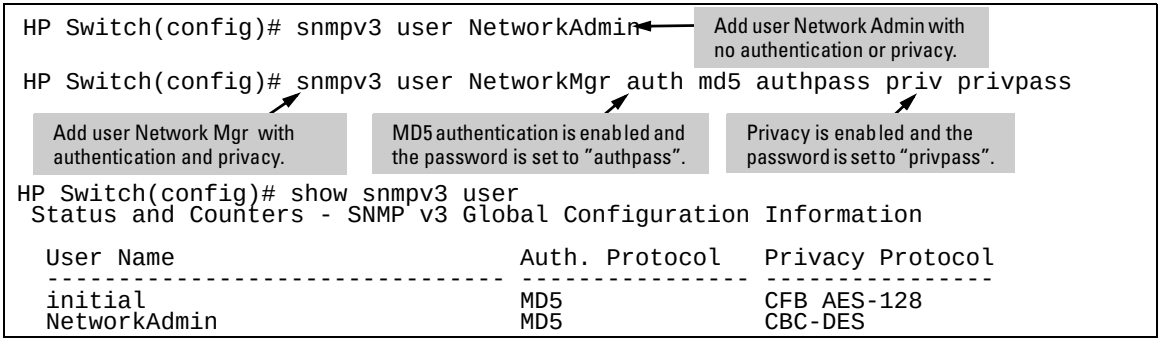



**Figure 5-2. Adding SNMPv3 Users and Displaying SNMPv3 Configuration**

### SNMPv3 User Commands

***Syntax:*** [no] snmpv3 user *<user_name>*

*Adds or deletes a user entry for SNMPv3. Authorization and privacy are optional, but to use privacy, you must use authorization. When you delete a user, only the <user_name> is required.*

[auth <md5 | sha> *<auth_pass>*]

*With authorization, you can set either MD5 or SHA authentication. The authentication password <auth_pass> must be 6-32 characters in length and is mandatory when you configure authentication.*
*Default: None*

[priv <des | aes> *<priv_pass>*]

*With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption. The privacy password <priv_pass> must be 6-32 characters in length and is mandatory when you configure privacy.*
*Default: DES*

***Note***: *Only AES 128-bit and DES 56-bit encryption are supported as privacy protocols. Other non-standard encryption algorithms, such as AES-172, AES-256, and 3-DES are not supported.*

**Listing Users.** To display the management stations configured to access the switch with SNMPv3 and view the authentication and privacy protocols that each station uses, enter the **show snmpv3 user** command.

***Syntax:*** show snmpv3 user

This example displays information about the management stations configured on VLAN 1 to access the switch.

```
HP Switch# configure terminal
HP Switch(config)# vlan 1
HP Switch(config)# show snmpv3 user

 Status and Counters - SNMP v3 Global Configuration Information

  User Name                       Auth. Protocol   Privacy Protocol
  ------------------------------- ---------------- ----------------
  initial                         MD5              CFB AES-128
  NetworkAdmin                    MD5              CBC-DES
```

**Figure 5-3. Example of Management Station Information**

**Assigning Users to Groups.** Then you must set the group access level for the user by assigning the user to a group. This is done with the **snmpv3 group** command. For more details on the MIBs access for a given group refer to "Group Access Levels" on page 5-8.

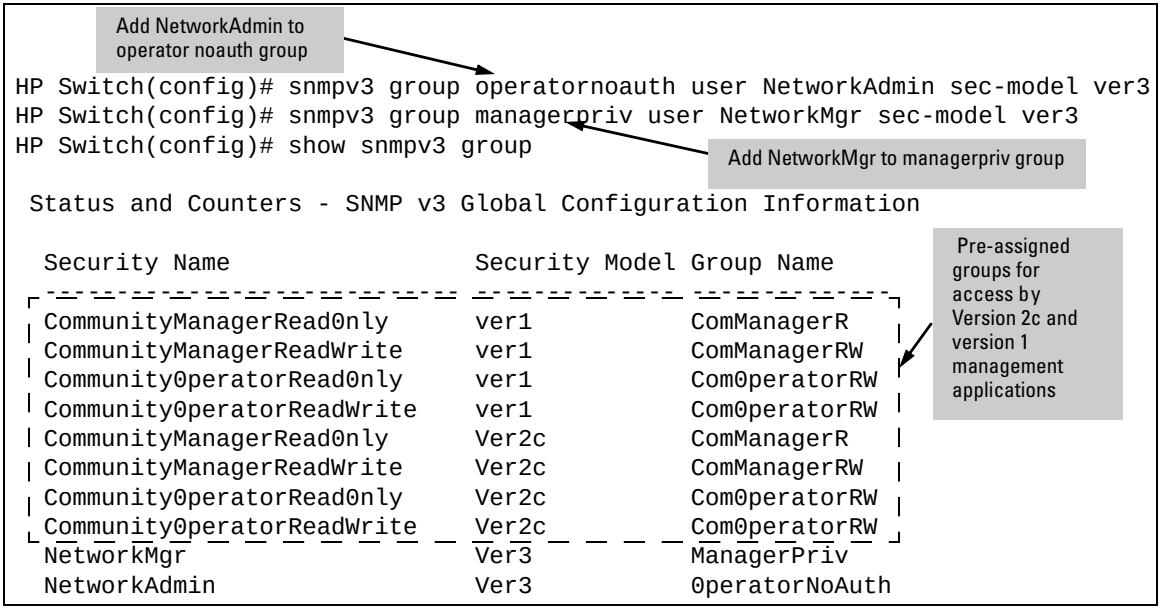



**Figure 5-4. Example of Assigning Users to Groups**

### SNMPv3 Group Commands

***Syntax:*** [no] snmpv3 group

*This command assigns or removes a user to a security group for access rights to the switch. To delete an entry, all of the following three parameters must be included in the command.*

group *<group_name>*

*This parameter identifies the group that has the privileges that will be assigned to the user. For more details refer to "Group Access Levels" on page 5-8.*

user *<user_name>*

*This parameter identifies the user to be added to the access group. This must match the user name added with the* **snmpv3 user** *command.*

sec-model <ver1 | ver2c | ver3>

*This defines which security model to use for the added user. A SNMPv3 access Group should only use the ver3 security model.*

## Group Access Levels

The switch supports eight predefined group access levels. There are four levels for use with version 3 users and four are used for access by version 2c or version 1 management applications.

| Group Name | Group Access Type | Group Read View | Group Write View |
|---|---|---|---|
| managerpriv | Ver3 Must have Authentication and Privacy | ManagerReadView | ManagerWriteView |
| managerauth | Ver3 Must have Authentication | ManagerReadView | ManagerWriteView |
| operatorauth | Ver3 Must have Authentication | OperatorReadView | DiscoveryView |
| operatornoauth | Ver3 No Authentication | OperatorReadView | DiscoveryView |
| commanagerrw | Ver2c or Ver1 | ManagerReadView | ManagerWriteView |
| commanagerr | Ver2c or Ver1 | ManagerReadView | DiscoveryView |
| comoperatorrw | Ver2c or Ver1 | OperatorReadView | OperatorReadView |
| comoperatorr | Ver2c or Ver1 | OperatorReadView | DiscoveryView |

Each view allows you to view or modify a different set of MIBs.

- **Manager Read View** – access to all managed objects
- **Manager Write View** – access to all managed objects *except* the following: vacmContextTable, vacmAccessTable, vacmViewTreeFamilyTable

- **OperatorReadView** – no access to icfSecurityMIB, hpSwitchIpTftp-Mode, vacmContextTable, vacmAccessTable, vacmViewTreeFamily-Table, usmUserTable, snmpCommunityTable
- **Discovery View** – Access limited to samplingProbe MIB.

**Note** All access groups and views are predefined on the switch. There is no method to modify or add groups or views to those that are pre-defined on the switch.

## SNMPv3 Communities

SNMP commuities are supported by the switch to allow management applications that use version 2c or version 1 to access the switch. The communities are mapped to Group Access Levels that are used for version 2c or version 1 support. For more information refer to "Group Access Levels" on page 5-8. This mapping will happen automatically based on the communities access privileges, but special mappings can be added with the **snmpv3 community** command.

***Syntax:*** [no] snmpv3 community

*This command maps or removes a mapping of a community name to a group access level. To remove a mapping you, only need to specify the* ***index_name*** *parameter.*

index *<index_name>*

*This is an index number or title for the mapping. The values of 1-5 are reserved and can not be mapped.*

name *<community_name>*

*This is the community name that is being mapped to a group access level.*

sec-name *<security_name>*

*This is the group level to which the community is being mapped. For more information refer to "Group Access Levels" on page 5-8.*

tag *<tag_value>*

*This is used to specify which target address may have access by way of this index reference.*

Figure 5-5 shows the assigning of the Operator community on MgrStation1 to the CommunityOperatorReadWrite group. Any other Operator only has an access level of CommunityOperatorReadOnly

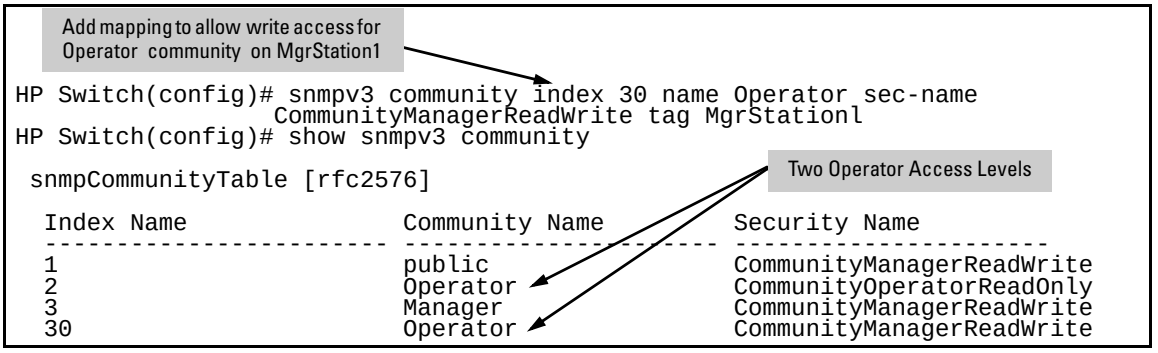



**Figure 5-5. Assigning a Community to a Group Access Level**

### SNMP Community Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| show SNMP communities | n/a | page 5-11 | page 5-12 | — |
| configure identity information | none | — | page 5-13 | |
| configure community names | public | page 5-11 | page 5-13 | — |
| MIB view for a community name (operator, manager) | manager | " | " | |
| write access for default community name | unrestricted | " | " | |

Use SNMP communities to restrict access to the switch by SNMP management stations by adding, editing, or deleting SNMP communities. You can configure up to five SNMP communities, each with either an operator-level or a manager-level view, and either restricted or unrestricted write access.

Using SNMP requires that the switch have an IP address and subnet mask compatible with your network.

**Caution**

For PCM version 1.5 or earlier (or any TopTools version), deleting the "public" community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and you are using the above software versions, HP recommends that you change the write access for the "public" community to "Restricted".

## Menu: Viewing and Configuring non-SNMP version 3 Communities

**To View, Edit, or Add SNMP Communities:**

1. From the Main Menu, Select:
   **2. Switch Configuration...**
   **6. SNMP Community Names**

**Note:** This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

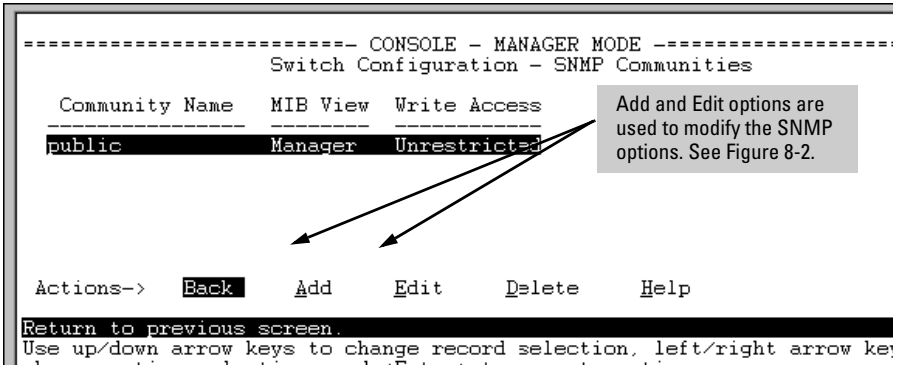



**Figure 5-6. The SNMP Communities Screen (Default Values)**

2. Press **[A]** (for **Add**) to display the following screen:

If you are adding a community, the fields in this screen are blank.

If you are editing an existing community, the values for the currently selected Community appear in the fields.

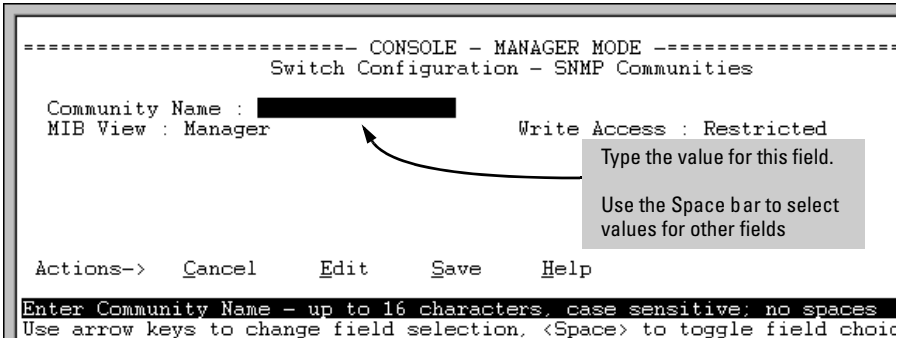



**Figure 5-7. The SNMP Add or Edit Screen**

**Need Help?** If you need information on the options in each field, press **[Enter]** to move the cursor to the Actions line, then select the **Help** option on the Actions line. When you are finished with Help, press **[E]** (for Edit) to return the cursor to the parameter fields.

3. Enter the name you want in the Community Name field, and use the Space bar to select the appropriate value in each of the other fields. (Use the **[Tab]** key to move from one field to the next.)
4. Press **[Enter]**, then **[S]** (for **Save**).

## CLI: Viewing and Configuring SNMP Community Names

| Community Name Commands | Page |
|---|---|
| show snmp-server [<*community-string*>] | 5-12 |
| [no] snmp-server | 5-13 |
| [community <*community-str*>] | 5-13 |
| [host <*community-str*> <*ip-addr*>] [<none \| debug \| all \| not-info \| critical>] | 5-16 |
| [enable traps <authentication> | 5-23 |
| [enable traps link-change <port-list>] | 5-24 |

**Listing Community Names and Values.** This command lists the data for currently configured SNMP community names (along with trap receivers and the setting for authentication traps — refer to "SNMP Notifications" on page 5-14).

***Syntax:*** show snmp-server [<*community-string*>]

This example lists the data for all communities in a switch; that is, both the default "public" community name and another community named "blue-team"

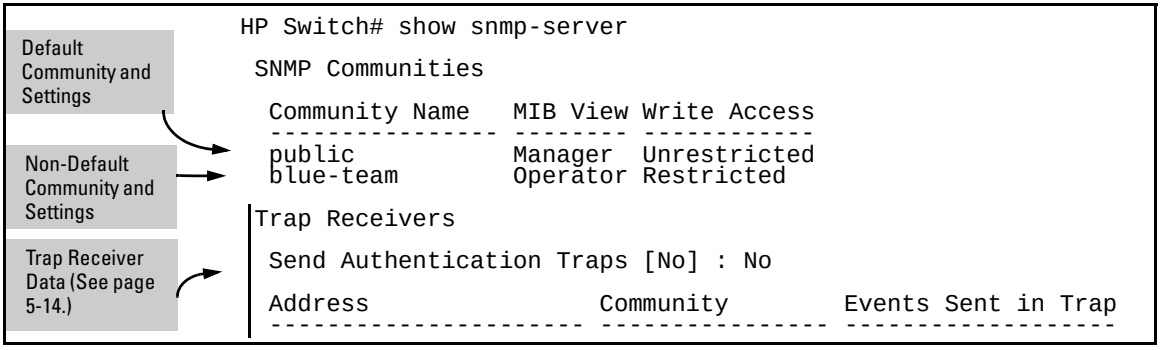



**Figure 5-8. Example of the SNMP Community Listing with Two Communities**

To list the data for only one community, such as the "public" community, use the above command with the community name included. For example:

```
HP Switch# show snmp-server public
```

**Configuring Community Names and Values.** The **snmp-server** command enables you to add SNMP communities with either default or specific access attributes, and to delete specific communities.

***Syntax:*** [no] snmp-server community < *community-name* >

Configures a new community name. If you do not also specify **operator** or **manager**, the switch automatically assigns the community to the **operator** MIB view. If you do not specify **restricted** or **unrestricted**, the switch automatically assigns the community to **restricted** (read-only) access. The **no** form uses only the **< community-name >** variable and deletes the named community from the switch.

[operator | manager]

*Optionally assigns an access level. At the* **operator** *level the community can access all MIB objects except the CONFIG MIB. At the* **manager** *level the community can access all MIB objects.*

[restricted | unrestricted]

*Optionally assigns MIB access type. Assigning the* **restricted** *type allows the community to read MIB variables, but not to set them. Assigning the* **unrestricted** *type allows the community to read and set MIB variables.*

For example, to add the following communities:

| Community | Access Level | Type of Access |
|---|---|---|
| red-team | manager *(Access to all MIB objects.)* | unrestricted *(read/write)* |
| blue-team | operator *(Access to all MIB objects except the CONFIG MIB.)* | restricted *(read-only)* |

```
HP Switch(config)# snmp-server community red-team
      manager unrestricted
HP Switch(config)# snmp-server community blue-team
      operator restricted
```

To eliminate a previously configured community named "gold-team":

```
HP Switch(config) # no snmp-server community gold-team
```

# SNMP Notifications

The switches covered in this guide support:

- SNMP version 1 or SNMP version 2c traps
- SNMPv2c informs
- SNMPv3 notification process, including traps

This section describes how to configure a switch to send network security and link-change notifications to configured trap receivers.

## Supported Notifications

By default, the following notifications are enabled on a switch:

- Manager password changes
- SNMP authentication failure
- Link-change traps: when the link on a port changes from up to down (linkDown) or down to up (linkUp)
- Port-security (web, MAC, or 802.1X) authentication failure
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Inability to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- ARP protection events

In addition, you can enable the switch to send the following types of notifications to configured trap receivers. For information on how to configure each notification, refer to the HP software guide under which the notification is listed.

- *Management and Configuration Guide:*
  - Configuration changes
  - Link-Layer Discovery Protocol (LLDP)
  - Ping tests
  - Power over Ethernet (POE): port toggle, power limit
  - RMON
- *Advance Traffic Management Guide:*
  - Loop protection
  - Spanning Tree (STP, RSTP, MSTP)

- *Access Security Guide:*
  - MAC lockdown
  - MAC lockout

## General Steps for Configuring SNMP Notifications

To configure SNMP notifications, follow these general steps:

1. Determine the versions of SNMP notifications that you want to use in your network.

   If you want to use SNMPv1 and SNMPv2c traps, you must also configure a trap receiver. Refer to the following sections and follow the required configuration procedures:
   - "SNMPv1 and SNMPv2c Traps" on page 5-16
   - "Configuring an SNMP Trap Receiver" on page 5-16
   - "Enabling SNMPv2c Informs" on page 5-18

   If you want to use SNMPv3 notifications (including traps), you must also configure an SNMPv3 management station. Follow the required configuration procedure in the following section:
   - "Configuring SNMPv3 Notifications" on page 5-19
2. To reconfigure any of the SNMP notifications that are enabled by default to be sent to a management station (trap receiver), refer to these sections:
   - "Enabling Link-Change Traps" on page 5-24
3. (Optional) Refer to the following sections to configure optional SNMP notification features and verify the current configuration:
   - "Configuring the Source IP Address for SNMP Notifications" on page 5-25
   - "Displaying SNMP Notification Configuration" on page 5-27

## SNMPv1 and SNMPv2c Traps

The switches covered in this guide support the following functionality from earlier SNMP versions (SNMPv1 and SNMPv2c):

- **Trap receivers:** A *trap receiver* is a management station to which the switch sends SNMP traps and (optionally) event log messages sent from the switch. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch.
- **Fixed or "Well-Known" Traps:** A switch automatically sends fixed traps (such as "coldStart", "warmStart", "linkDown", and "linkUp") to trap receivers using a **public** or **non-public** community name.
- **Thresholds:** A switch automatically sends all messages created when a system threshold is reached to the network management station that configured the threshold, regardless of the trap receiver configuration.

## Configuring an SNMP Trap Receiver

Use the **snmp-server host** command to configure a trap receiver that can receive SNMPv1 and SNMPv2c traps, and (optionally) event log messages. When you configure a trap receiver, you specify its community membership, management station IP address, and (optionally) the type of event log messages to be sent.

If you specify a community name that does not exist—that is, has not yet been configured on the switch—the switch still accepts the trap receiver assignment. However, no traps will be sent to that trap receiver until the community to which it belongs has been configured on the switch.

***Syntax:*** snmp-server host <*ipv4-addr* | *ipv6-addr*> <*community name*>

*Configures a destination network management station to receive SNMPv1/v2c traps, and (optionally) event log messages sent as traps from the switch, using the specified community name and destination IPv4 or IPv6 address. You can specify up to ten trap receivers (network management stations). The default community name is* **public**.

[<none | all | non-info | critical | debug>]

*(Optional) Configures the security level of the event log messages you want to send as traps to a trap receiver (see table 5-1, "Security Levels for Event Log Messages Sent as Traps").*

- *The type of event log message that you specify applies only to event log messages, not to threshold traps.*
- *For each configured event level, the switch continues to send threshold traps to all network management stations that have the appropriate threshold level configured.*
- *If you do not specify an event level, the switch uses the default value (***none***) and sends no event log messages as traps.*

[<inform>]

*(Optional) Configures the switch to send SNMPv2 inform requests when certain events occur. See "Enabling SNMPv2c Informs" on page 5-18 for more information.*

**Table 5-1. Security Levels for Event Log Messages Sent as Traps**

| Security Level | Action |
|---|---|
| None (default) | Sends no event log messages. |
| All | Sends all event log messages. |
| Non-Info | Sends all event log messages that are not for information only. |
| Critical | Sends only event log messages for critical error conditions. |
| Debug | Sends only event log messages needed to troubleshoot network- and switch-level problems. |

For example, to configure a trap receiver in a community named "red-team" with an IP address of 10.28.227.130 to receive only "critical" event log messages, you can enter the following command:

```
HP Switch(config)# snmp-server host 10.28.227.130 red-
team critical
```

## Notes

To replace one community name with another for the same IP address, you must first enter the **no snmp-server host** < *community-name*> <*ipv4-address* | *ipv6-address* > command to delete the unwanted community name. Otherwise, if

you add a new community name with an IP address that is already used with a different community name, two valid community name entries are created for the same management station.

If you do not specify the event level ([<none | all | non-info | critical | debug>]), the switch does not send event log messages as traps. However, "well-known" traps and threshold traps (if configured) are still sent.

## Enabling SNMPv2c Informs

On a switch enabled for SNMPv2c, you can use the **snmp-server host inform** command to send inform requests when certain events occur. When an SNMP Manager receives an inform request, it can send an SNMP response back to the sending agent on the switch to let the agent know that the inform request reached its destination.

If the sending agent on the switch does not receive an SNMP response back from the SNMP Manager within the timeout period, the inform request may be resent, based on the retry count value.

When you enable SNMPv2c inform requests to be sent, you must specify the IP address and community name of the management station that will receive the inform notification.

***Syntax:*** [no] snmp-server host <*ipv4-addr* | *ipv6-addr*> <*community name*> inform [retries <*count*>] [timeout <*interval*>]]

*Enables (or disables) the* ***inform*** *option for SNMPv2c on the switch and allows you to configure options for sending SNMP inform requests.*

**retries:** *Maximum number of times to resend an inform request if no SNMP response is received. Default: 3*

**timeout:** *Number of seconds to wait for an acknowledgement before resending the inform request. Default: 15 seconds*

**Note** The **retries** and **timeout** values are not used to send trap requests.

To verify the configuration of SNMPv2c informs, enter the **show snmp-server** command:

```
HP Switch(config)# show snmp-server

 SNMP Communities

  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  ...

  Address               Community       Events Sent Notify Type Retry Timeout
  --------------------- --------------- ----------- ----------- ----- --------
  12.28.333.456         guest           All         inform      3     15

 Excluded MIBs

 Snmp Response Pdu Source-IP Information

  Selection Policy   : Default rfc1517

 Trap Pdu Source-IP Information
  Selection Policy   : Configured IP
  Ip Address         : 10.10.10.10
```

SNMPv2c Inform configuration

**Figure 5-9. Display of SNMPv2c Inform Configuration**

## Configuring SNMPv3 Notifications

The SNMPv3 notification process allows messages that are passed via SNMP between the switch and a network management station to be authenticated and encrypted.

To configure SNMPv3 notifications, follow these steps:

1. Enable SNMPv3 operation on the switch by entering the **snmpv3 enable** command (see “SNMP Version 3 Commands” on page 5-4).

   When SNMPv3 is enabled, the switch supports:

   - Reception of SNMPv3 notification messages (traps and informs)
   - Configuration of initial users
   - (Optional) Restriction of non-SNMPv3 messages to “read only”

2. Configure SNMPv3 users by entering the **snmpv3 user** command (see “SNMPv3 Users” on page 5-5). Each SNMPv3 user configuration is entered in the User Table.

3. Assign SNMPv3 users to security groups according to their level of access privilege by entering the **snmpv3 group** command (see "Assigning Users to Groups" on page 5-7).

4. Define the name of an SNMPv3 notification configuration by entering the **snmpv3 notify** command.

***Syntax:*** [no] snmpv3 notify <*notify_name*> tagvalue <*tag_name*>

*Associates the name of an SNMPv3 notification configuration with a tag name used (internally) in SNMPv3 commands. To delete a notification-to-tag mapping, enter* **no snmpv3 notify <*notify_name*>**.

notify < *notify_name* >

*Specifies the name of an SNMPv3 notification configuration.*

tagvalue < *tag_name* >

*Specifies the name of a tag value used in other SNMPv3 commands, such as* **snmpv3 targetaddress params taglist** *<tag_name> in Step 5.*

5. Configure the target address of the SNMPv3 management station to which SNMPv3 informs and traps are sent by entering the **snmpv3 targetaddress** command.

***Syntax:*** [no] snmpv3 targetaddress < *ipv4-addr* | *ipv6-addr*> < *name* >

*Configures the IPv4 or IPv6 address, name, and configuration filename of the SNMPv3 management station to which notification messages are sent.*

params < *parms_name* >

*Name of the SNMPv3 station's parameters file. The parameters filename configured with* **params** *<params_name> must match the* **params** *<params_name> value entered with the* **snmpv3 params** *command in Step 6.*

taglist <*tag_name*> [*tag_name*] ...

*Specifies the SNMPv3 notifications (identified by one or more <tag_name> values) to be sent to the IP address of the SNMPv3 management station.*

*You can enter more than one <tag_name> value. Each <tag_name> value must be already associated with the name of an SNMPv3 notification configuration entered with the* **snmpv3 notify** *command in Step 4.*

*Use a blank space to separate <tag_name> values.*

*You can enter up to 103 characters in <tag_name> entries following the* **taglist** *keyword.*

[filter < none | debug | all | not-info | critical>]

*(Optional) Configures the type of messages sent to a management station. Default:* **none**.

[udp-port < *port* >]

*(Optional) Specifies the UDP port to use. Default:* **162**.

[port-mask < *mask* >]

*(Optional) Specifies a range of UDP ports. Default:* **0**.

[addr-mask < *mask* >]

*(Optional) Specifies a range of IP addresses as destinations for notification messages. Default:* **0**.

[retries < *value* >]

*(Optional) Number of times a notification is retransmitted if no response is received. Range: 1-255. Default:* **3.**

[timeout < *value* >]

*(Optional) Time (in millisecond increments) allowed to receive a response from the target before notification packets are retransmitted. Range: 0-2147483647. Default:* **1500** *(15 seconds).*

[max-msg-size<*size*>]

*(Optional) Maximum number of bytes supported in a notification message to the specified target. Default:* **1472**

Create a configuration record for the target address with the **snmpv3 params** command.

***Syntax*** [no] snmpv3 params *<params_name>* user *<user_name>*

*Applies the configuration parameters and IP address of an SNMPv3 management station (from the* **params** *<params_name> value configured with the* **snmpv3 targetaddress** *command in Step 5) to a specified SNMPv3 user (from the* **user** *<user_name> value configured with the* **snmpv3 user** *command in Step 2).*

*If you enter the* **snmpv3 params user** *command, you must also configure a security model (***sec-model***) and message processing algorithm (***msg-processing***).*

< sec-model < ver1 | ver2c | ver3 >

*Configures the security model used for SNMPv3 notification messages sent to the management station configured with the* **snmpv3 targetaddress** *command in Step 5.*

*If you configure the security model as* **ver3**, *you must also configure the message processing value as* **ver3**.

< msg-processing < ver1 | ver2c | ver3 > [noaut | auth | priv]

*Configures the algorithm used to process messages sent to the SNMPv3 target address.*

*If you configure the message processing value as* **ver3** *and the security model as* **ver3,** *you must also configure a security services level (***noauth**, **auth**, *or* **priv***).*

An example of how to configure SNMPv3 notification is shown here:

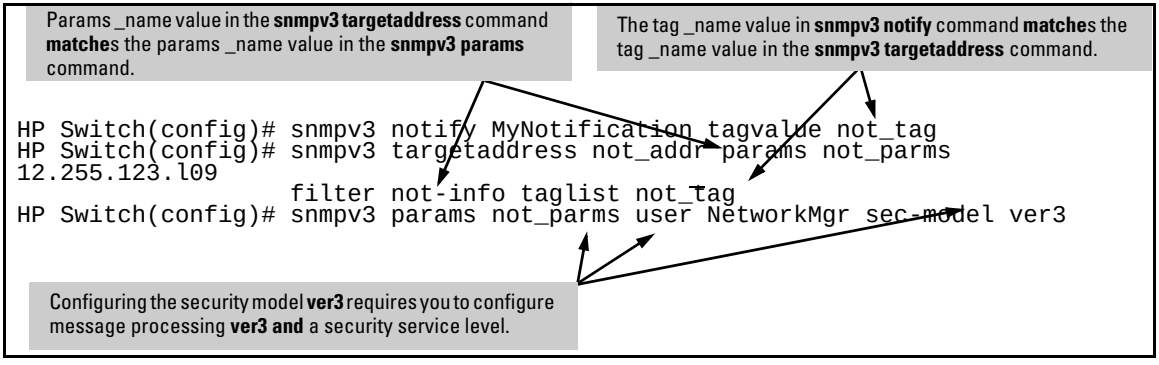



**Figure 5-10. Example of an SNMPv3 Notification Configuration**

## Managing Network Security Notifications

By default, a switch is enabled to send the SNMP notifications listed in "Supported Notifications" on page 5-14 when a network security event (for example, authentication failure) occurs. However, before security notifications can be sent, you must first configure one or more trap receivers or SNMPv3 management stations as described in:

- "Configuring an SNMP Trap Receiver" on page 5-16
- "Configuring SNMPv3 Notifications" on page 5-19

You can manage the default configuration of the switch to disable and re-enable notifications to be sent for the following types of security events:

- ARP protection events
- Unable to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- Link change notification
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Manager password changes
- Port-security (web, MAC, or 802.1X) authentication failure
- SNMP authentication failure

To enable or disable notification/traps for network security failures and other security events, enter the **snmp-server enable traps** command.

***Syntax:*** [no] snmp-server enable traps [snmp-auth | password-change-mgr | login-failure-mgr | port-security | auth-server-fail | link-change]

*Enables or disables sending one of the security notification types listed below to configured trap receivers. (Unless otherwise stated, all of the following notifications are enabled in the default configuration.*

- **auth-server-fail** sends a trap if the connection with a RADIUS or TACACS+ authentication server fails.
- **link-change < *port-list* >** sends a trap when the link state on a port changes from up to down, or the reverse.
- **login-failure-mgr** sends a trap for a failed login with a manager password.
- **password-change-mgr** sends trap when manager password is reset.
- **port-security** sends a trap for a failed authentication attempt through a web, MAC, or 801.X authentication session.
- **snmp-authentication [ extended | standard ]** sends a trap for a failed authentication attempt via SNMP. Default: **extended**.

To determine the specific cause of a security event, check the event log in the console interface to see why a trap was sent. For more information, refer to "Using the Event Log for Troubleshooting Switch Problems" on page C-17.

To display the current configuration for network security notifications, enter the **show snmp-server traps** command. Note that command output is a subset of the information displayed with the **show snmp-server** command in Figure 5-13.

```
HP Switch(config)# show snmp-server traps

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : 1-24

  Traps Category                    Current Status
  ------------------------------    --------------------------
  SNMP Authentication             : Extended
  Password change                 : Enabled
  Login failures                  : Enabled
  Port-Security                   : Enabled
  Authorization Server Contact    : Enabled

  Address                 Community   Events Sent  Type         Retry  Timeout
  ----------------------  ----------  -----------  -----------  -----  -------
  12.255.5.225            public      All          trap           3    15
  2001:0db8:0000:0001
    :0000:0000:0000:0121  user_1      All          trap           3    15

  Excluded MIBs
```

Link-change trap setting

**Figure 5-11. Display of Configured Network Security Notifications**

## Enabling Link-Change Traps

By default a switch is enabled to send a trap when the link state on a port changes from up to down (linkDown) or down to up (linkUp). To reconfigure the switch to send link-change traps to configured trap receivers, enter the **snmp-server enable traps link-change** command.

***Syntax:*** [no] snmp-server enable traps link-change<*port-list*> [all]

*Enables or disables the switch to send a link-change trap to configured trap receivers when the link state on a port goes from up to down or down to up.*
*Enter* **all** *to enable or disable link-change traps on all ports on the switch.*

## Configuring the Source IP Address for SNMP Notifications

The switch uses an interface IP address as the source IP address in IP headers when sending SNMP notifications (traps and informs) or responses to SNMP requests.

For multi-netted interfaces, the source IP address is the IP address of the outbound interface of the SNMP reply, which may differ from the destination IP address in the IP header of the received request. For security reasons, it may be desirable to send an SNMP reply with the IP address of the destination interface (or a specified IP address) on which the corresponding SNMP request was received.

To configure the switch to use the source IP address on which an SNMP request was received in SNMP notification/traps and replies, enter the **snmp-server response-source** and **snmp-server trap-source** commands.

***Syntax:*** [no] snmp-server response-source [dst-ip-of-request | <*ip-addr*>]

*Specifies the source IP address of the SNMP response PDU. The default SNMP response PDU uses the IP address of the active interface from which the SNMP response was sent as the source IP address.*
*The* **no** *form of the command resets the switch to the default behavior (compliant with rfc-1517).*
*Default: Interface IP address*

**dst-ip-of-request:** *Destination IP address of the SNMP request PDU that is used as the source IP address in an SNMP response PDU.*

**<***ip-addr***>**: *User-defined interface IP address that is used as the source IP address in an SNMP response PDU.*

For example, to use the IP address of the destination interface on which an SNMP request was received as the source IP address in the IP header of SNMP traps and replies, enter the following command:

```
HP Switch(config)# snmp-server response-source
dst-ip-of-request
```

To configure the switch to use a specified source IP address in generated trap PDUs, enter the **snmp-server trap-source** command.

***Syntax:*** [no] snmp-server trap-source [<*ipv4-addr* >]

*Specifies the source IP address to be used for a trap PDU. The* **no** *form of the command resets the switch to the default behavior (compliant with rfc-1517).*
*Default: Use the interface IP address in generated trap PDUs.*

**<***ipv4-addr***>**: *User-defined interface IPv4 address that is used as the source IP address in generated traps. IPv6 addresses are not supported.*

## Notes

When you use the **snmp-server response-source** and **snmp-server trap-source** commands, note the following behavior:

- The **snmp-server response-source** and **snmp-server trap-source** commands configure the source IP address for IPv4 interfaces only.
- You must manually configure the **snmp-server response-source** value if you wish to change the default user-defined interface IP address that is used as the source IP address in SNMP traps (RFC 1517).
- The values configured with the **snmp-server response-source** and **snmp-server trap-source** commands are applied globally to all interfaces that are sending SNMP responses or SNMP trap PDUs.
- Only the source IP address field in the IP header of the SNMP response PDU can be changed.
- Only the source IP address field in the IP header and the SNMPv1 Agent Address field of the SNMP trap PDU can be changed.

To verify the configuration of the interface IP address used as the source IP address in IP headers for SNMP replies and traps sent from the switch, enter the **show snmp-server** command to display the SNMP policy configuration.

```
HP Switch(config)# show snmp-server
 SNMP Communities
  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Manager  Unrestricted
 Trap Receivers
  Link-Change Traps Enabled on Ports [All] : All
  ...
 Excluded MIBs
 Snmp Response Pdu Source-IP Information
  Selection Policy   : dstIpOfRequest
 Trap Pdu Source-IP Information
  Selection Policy   : Configured IP
```

**dstIpOfRequest**: The destination IP address of the interface on which an SNMP request is received i s used as the source IP address in SNMP replies.

**Figure 5-12. Display of Source IP Address Configuration**

## Displaying SNMP Notification Configuration

Use the **show snmp-server** command to display the currently configured:

- Management stations (trap receivers)
- Settings for network security notifications and link-change traps
- SNMP communities

***Syntax:*** show snmp-server

*Displays the currently configured notification settings for versions SNMPv1 and SNMPv2c traps, including SNMP communities, trap receivers, link-change traps, and network security notifications.*

In the following example, the **show snmp-server** command output shows that the switch has been configured to send SNMP traps and notifications to management stations that belong to the "public", "red-team", and "blue-team" communities.

```
HP Switch(config)# show snmp-server
 SNMP Communities
  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Operator Restricted
  blue-team        Manager  Unrestricted
  red-team         Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Trap Category                    Current Trap Configuration
  -------------------------------  --------------------------
  SNMP Authentication              extended
  Password change                  enabled
  Login failures                   enabled
  Port-Security                    enabled
  Authorization Server Contact     enabled

  Address          Community   Events Sent  Notify Type  Retry  Timeout
  ---------------  ----------  -----------  -----------  -----  -------
  10.28.227.200    public      All          trap           3      15
  10.28.227.105    red-team    Critical     trap           3      15
  10.28.227.120    blue-team   Not-INFO     trap           3      15
...
```

SNMP Community configuration

Link-change trap setting

**Figure 5-13. Display of SNMP Notification Configuration**

## Advanced Management: RMON

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

The following RMON groups are supported:

- Ethernet Statistics (except the numbers of packets of different frame sizes)
- Alarm
- History (of the supported Ethernet statistics)
- Event

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events. Note that you can access the Ethernet statistics, Alarm, and Event groups from the IMC network management software. For more on IMC, visit the HP web site at

**www.hp.com/Networking**

Navigate to Network management.

## CLI-Configured sFlow with Multiple Instances

In earlier software releases, sFlow was configured on the switch via SNMP using a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to three distinct sFlow instances: once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. CLI-configured sFlow instances may be saved to the startup configuration to persist across a switch reboot.

### Terminology

**sFlow —** An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

**sFlow agent —** A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

**sFlow destination —** The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

## Configuring sFlow

The following sFlow commands allow you to configure sFlow instances via the CLI.

***Syntax:*** [no] sflow <*receiver-instance*> destination <*ip-address*> [*udp-port-num*]

*Enables an sFlow receiver/destination. The receiver-instance number must be a 1, 2, or 3. By default, the udp destination port number is 6343.*

*To disable an sFlow receiver/destination, enter no sflow <receiver-instance>.*

***Syntax:*** sflow <*receiver-instance*> sampling <*port-list*> <*sampling rate*>

*Once an sFlow receiver/destination has been enabled, this command enables flow sampling for that instance. The receiver-instance number is 1, 2, or 3, and the sampling rate is the allowable non-zero skipcount for the specified port or ports.*

*To disable flow-sampling for the specified port-list, repeat the above command with a sampling rate of "0".*

***Syntax:*** sflow <*receiver-instance*> polling <*port-list*> <*polling interval*>

*Once an sFlow receiver/destination has been enabled, this command enables counter polling for that instance. The receiver-instance number is 1, 2, or 3, and the polling interval may be set to an allowable non-zero value to enable polling on the specified port or ports.*

*To disable counter-polling for the specified port-list, repeat the above command with a polling interval of "0".*

**Note**

Under the multiple instance implementation, sFlow can be configured via the CLI or via SNMP. However, CLI-owned sFlow configurations cannot be modified via SNMP, whereas SNMP-owned instances can be disabled via the CLI using the **no sflow** <*receiver-instance*> command.

## Viewing sFlow Configuration and Status

The following sFlow commands allow you to display sFlow configuration and status via the CLI.

***Syntax:*** show sflow agent

*Displays sFlow agent information. The agent address is normally the ip address of the first vlan configured.*

***Syntax:*** show sflow <receiver instance> destination

*Displays information about the management station to which the sFlow sampling-polling data is sent.*

***Syntax:*** show sflow <receiver instance> sampling-polling <port-list/range>

*Displays status information about sFlow sampling and polling.*

The **show sflow agent** command displays read-only switch agent information. The version information shows the sFlow version, MIB support and software versions; the agent address is typically the ip address of the first vlan configured on the switch.

```
HP Switch# show sflow agent

  Version           1.3;HP;K.11.40
  Agent Address     10.0.10.228
```

**Figure 5-14. Example of Viewing sFlow Agent Information**

The **show sflow** <*instance*> **destination** command includes information about the management-station's destination address, receiver port, and owner.

```
HP Switch# show sflow 2 destination

  Destination Instance         2
  sflow                        Enabled
  Datagrams Sent               221
  Destination Address          10.0.10.41
  Receiver Port                6343
  Owner                        Administrator, CLI-owned, Instance 2
  Timeout (seconds)            99995530
  Max Datagram Size            1400
  Datagram Version Support     5
```

**Figure 5-15. Example of Viewing sFlow Destination Information**

Note the following details:

- **Destination Address** remains blank unless it has been configured.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.
- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

The **show sflow** <*instance*> **sampling-polling** [port-list] command displays information about sFlow sampling and polling on the switch. You can specify a list or range of ports for which to view sampling information.

```
HP Switch# show sflow 2 sampling-polling 1-4

                    Number denotes the sampling/polling instance to which the receiver is coupled.

 Port  | Sampling                        Dropped     |  Polling
       | Enabled  Rate     Header  Samples     |  Enabled  Interval
 ----- + -------- -------- ------  ----------  + -------  --------
  1      Yes(2)   40       128     1234567890     ---       ---
  2      ---      ---      ---             0     Yes(1)    60
  3      No(1)    0        100        898703     No        30
  4      Yes(3)   50       128             0     No(3)      0
```

**Figure 5-16. Example of Viewing sFlow Sampling and Polling Information**

**Note**

The sampling and polling instances (noted in parentheses) coupled to a specific receiver instance are assigned dynamically, and so the instance numbers may not always match. The key thing to note is whether sampling or polling is enabled on a port, and the sampling rates or polling intervals for the receiver instance configured on each port.

# LLDP (Link-Layer Discovery Protocol)

To standardize device discovery on all HP switches, LLDP will be implemented while offering limited read-only support for CDP as documented in this manual. For the latest information on your switch model, consult the Release Notes (available on the HP web site). If LLDP has not yet been implemented (or if you are running an older version of software), consult a previous version of the *Management and Configuration Guide* for device discovery details.

**Table 5-2. LLDP and LLDP-MED Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| View the switch's LLDP configuration | n/a | — | page 5-40 | — |
| Enable or disable LLDP on the switch | Enabled | — | page 5-35 | — |
| Change the transmit interval (refresh-interval) for LLDP packets | 30 seconds | — | page 5-43 | — |
| Change the holdtime multiplier for LLDP Packets (holdtime-multiplier x refresh-interval = time-to-live) | 4 seconds | — | page 5-36 | — |
| Change the delay interval between advertisements | 2 seconds | — | page 5-44 | — |
| Changing the reinitialization delay interval | 2 seconds | — | page 5-45 | — |
| Configuring SNMP notification support | Disabled | — | page 5-45 | — |
| Configuring transmit and receive modes | tx_rx | — | page 5-46 | — |
| Configuring basic LLDP per-port advertisement content | Enabled | — | page 5-47 | — |
| Configuring port speed and duplex advertisements for optional LLDP and mandatory LLDP-MED applications | Enabled | — | page 5-65 | — |
| Configuring topology change notification for LLDP-MED | Enable | — | page 5-52 | — |
| Changing the fast-start duration for LLDP-MED | 5 sec | — | page 5-54 | |
| Configuring LLDP-MED Advertising | Enabled | — | page 5-47 | |
| Configuring LLDP-MED device location data | None | — | page 5-63 | |
| Displaying Advertisement Data and Statistics | n/a | — | page 5-67 | — |

**LLDP (Link Layer Discovery Protocol):** provides a standards-based method for enabling the switches covered in this guide to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

**LLDP-MED (LLDP Media Endpoint Discovery):** Provides an extension to LLDP and is designed to support VoIP deployments.

**Note** LLDP-MED is an extension for LLDP, and the switch requires that LLDP be enabled as a prerequisite to LLDP-MED operation.

An SNMP utility can progressively discover LLDP devices in a network by:

1. Reading a given device's Neighbors table (in the Management Information Base, or MIB) to learn about other, neighboring LLDP devices.
2. Using the information learned in step 1 to find and read the neighbor devices' Neighbors tables to learn about additional devices, and so on.

Also, by using **show** commands to access the switch's neighbor database for information collected by an individual switch, system administrators can learn about other devices connected to the switch, including device type (capability) and some configuration information. In VoIP deployments using LLDP-MED on the switches covered in this guide, additional support unique to VoIP applications is also available. Refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.

## Terminology

**Adjacent Device:** Refer to "Neighbor or Neighbor Device".

**Advertisement:** See LLDPDU.

**Active Port:** A port linked to another active device (regardless of whether MSTP is blocking the link).

**ELIN (Emergency Location Identification Number):** A valid telephone number in the North American Numbering Plan format and assigned to a multiline telephone system operator by the appropriate authority. This number calls a public service answering point (PSAP) and relays automatic location identification data to the PSAP.

**LLDP:** Link Layer Discovery Protocol:

- Switches covered in this guide: IEEE 802.1AB

**LLDP-Aware:** A device that has LLDP in its operating code, regardless of whether LLDP is enabled or disabled.

**LLDP Device:** A switch, server, router, or other device running LLDP.

**LLDP Neighbor:** An LLDP device that is either directly connected to another LLDP device or connected to that device by another, non-LLDP Layer 2 device (such as a hub) Note that an 802.1D-compliant switch does not forward LLDP data packets even if it is not LLDP-aware.

**LLDPDU (LLDP Data Unit):** LLDP data packet are transmitted on active links and include multiple TLVs containing global and per-port switch information. In this guide, LLDPDUs are termed “advertisements” or “packets”.

**LLDP-MED (Link Layer Discover Protocol Media Endpoint Discovery):** The TIA telecommunications standard produced by engineering subcommittee TR41.4, “VoIP Systems — IP Telephony infrastructure and Endpoints” to address needs related to deploying VoIP equipment in IEEE 802-based environments. This standard will be published as ANSI/TIA-1057.

**MIB** (Management Information Base): An internal database the switch maintains for configuration and performance information.

**MLTS (Multiline Telephone System):** A network-based and/or premises-based telephone system having a common interface with the public switched telephone system and having multiple telephone lines, common control units, multiple telephone sets, and control hardware and software.

**NANP (North American Numbering Plan):** A ten-digit telephone number format where the first three digits are an area code and the last seven-digits are a local telephone number.

**Neighbor:** See “LLDP Neighbor”.

**Non-LLDP Device:** A device that is not capable of LLDP operation.

**PD (Powered Device):** This is an IEEE 802.3af-compliant device that receives its power through a direct connection to a 10/100Base-TX PoE RJ-45 port in a HP fixed-port or chassis-based switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.

**PSAP (Public Safety Answering Point):** PSAPs are typically emergency telephone facilities established as a first point to receive emergency (911) calls and to dispatch emergency response services such as police, fire and emergency medical services.

**PSE (Power-Sourcing Equipment):** A PSE, such as a PoE port in a switch covered in this guide, provides power to IEEE 802.3af-compliant PDs directly connected to the ports.

**TLV (Type-Length-Value):** A data unit that includes a data type field, a data unit length field (in bytes), and a field containing the actual data the unit is designed to carry (as an alphanumeric string, a bitmap, or a subgroup of information). Some TLVs include subelements that occur as separate data

points in displays of information maintained by the switch for LLDP advertisements. (That is, some TLVs include multiple data points or subelements.)

## General LLDP Operation

An LLDP packet contains data about the transmitting switch and port. The switch advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets out all ports on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports that are inbound LLDP-enabled. (LLDP is a one-way protocol and does not include any acknowledgement mechanism.) An LLDP-enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

### LLDP-MED

This capability is an extension to LLDP and is available on the switches covered in this guide. Refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.

## Packet Boundaries in a Network Topology

- Where multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.
- An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Thus, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.
- Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

## Configuration Options

**Enable or Disable LLDP on the Switch.** In the default configuration, LLDP is globally enabled on the switch. To prevent transmission or receipt of LLDP traffic, you can disable LLDP operation (page 5-35)

**Enable or Disable LLDP-MED.** In the default configuration for the switches covered in this guide, LLDP-MED is enabled by default. (Requires that LLDP is also enabled.) For more information, refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.

**Change the Frequency of LLDP Packet Transmission to Neighbor Devices.** On a global basis, you can increase or decrease the frequency of outbound LLDP advertisements (page 5-36).

**Change the Time-To-Live for LLDP Packets Sent to Neighbors.** On a global basis, you can increase or decrease the time that the information in an LLDP packet outbound from the switch will be maintained in a neighbor LLDP device (page 5-36).

**Transmit and Receive Mode.** With LLDP enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions, and receives LLDP advertisements on each active port enabled to receive LLDP traffic (page 5-46). Per-Port configuration options include four modes:

- Transmit and Receive (**tx_rx**): This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets, and to store the data from received (inbound) LLDP packets in the switch's MIB.
- Transmit only (**txonly**): This setting enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
- Receive only (**rxonly**): This setting enables a port to receive and read LLDP packets from LLDP neighbors, and to store the packet data in the switch's MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.
- Disable (**disable**): This setting disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

**SNMP Notification.** You can enable the switch to send a notification to any configured SNMP trap receiver(s) when the switch detects a remote LLDP data change on an LLDP-enabled port (page 5-45).

**Per-Port (Outbound) Data Options.** The following table lists the information the switch can include in the per-port, outbound LLDP packets it generates. In the default configuration, all outbound LLDP packets include

this information in the TLVs transmitted to neighbor devices. However, you can configure LLDP advertisements on a per-port basis to omit some of this information (page 5-47).

**Table 5-3. Data Available for Basic LLDP Advertisements**

| Data Type | Configuration Options | Default | Description |
|---|---|---|---|
| Time-to-Live | See note 1. | 120 Seconds | The length of time an LLDP neighbor retains the advertised data before discarding it. |
| Chassis Type[2, 6] | N/A | Always Enabled | Indicates the type of identifier used for Chassis ID. |
| Chassis ID[6] | N/A | Always Enabled | Uses base MAC address of the switch. |
| Port Type[3, 6] | N/A | Always Enabled | Uses "Local", meaning assigned locally by LLDP. |
| Port Id[6] | N/A | Always Enabled | Uses port number of the physical port. In the switches covered in this guide, this is an internal number reflecting the reserved port position. For more information on this numbering scheme, refer to figures D-2 and D-3 in Appendix D, "MAC Address Management" of the *Management and Configuration Guide* for your switch. |
| Remote Management Address | | | |
| Type[4, 6] | N/A | Always Enabled | Shows the network address type. |
| Address[4] | Default or Configured | Uses a default address selection method unless an optional address is configured. See "Remote Management Address" on page 5-38. | |
| System Name[6] | Enable/Disable | Enabled | Uses the switch's assigned name. |
| System Description[6] | Enable/Disable | Enabled | Includes switch model name and running software version, and ROM version. |
| Port Description[6] | Enable/Disable | Enabled | Uses the physical port identifier. |
| System capabilities supported[5, 6] | Enable/Disable | Enabled | Identifies the switch's primary capabilities (bridge, router). |
| System capabilities enabled[5, 6] | Enable/Disable | Enabled | Identifies the primary switch functions that are enabled. |

[1]The Packet Time-to-Live value is included in LLDP data packets. (Refer to "Changing the Time-to-Live for Transmitted Advertisements" on page 5-43.)

[2]Subelement of the Chassis ID TLV.

[3]Subelement of the Port ID TLV.

[4]Subelement of the Remote-Management-Address TLV.

[5]Subelement of the System Capability TLV.

[6]Populated with data captured internally by the switch. For more on these data types, refer to the IEEE P802.1AB Standard.

**Remote Management Address.** The switch always includes an IP address in its LLDP advertisements. This can be either an address selected by a default process, or an address configured for inclusion in advertisements. Refer to "IP Address Advertisements" on page 5-39.

**Debug Logging.** You can enable LLDP debug logging to a configured debug destination (Syslog server and/or a terminal device) by executing the **debug lldp** command. (For more on Debug and Syslog, refer to the "Troubleshooting" appendix in this guide.) Note that the switch's Event Log does not record usual LLDP update messages.

## Options for Reading LLDP Information Collected by the Switch

You can extract LLDP information from the switch to identify adjacent LLDP devices. Options include:

- Using the switch's **show lldp info** command options to display data collected on adjacent LLDP devices—as well as the local data the switch is transmitting to adjacent LLDP devices (page 5-40).
- Using an SNMP application that is designed to query the Neighbors MIB for LLDP data to use in device discovery and topology mapping. 3400/6400 only?
- Using the **walkmib** command to display a listing of LLDP MIB objects

## LLDP and LLDP-MED Standards Compatibility

The operation covered by this section is compatible with these standards:

- IEEE P802.1AB
- RFC 2922 (PTOPO, or Physical Topology MIB)
- RFC 2737 (Entity MIB)
- RFC 2863 (Interfaces MIB)
- ANSI/TIA-1057/D6 (LLDP-MED; refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.)

## LLDP Operating Rules

(For additional information specific to LLDP-MED operation, refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.)

**Port Trunking.** LLDP manages trunked ports individually. That is, trunked ports are configured individually for LLDP operation, in the same manner as non-trunked ports. Also, LLDP sends separate advertisements on each port in a trunk, and not on a per-trunk basis. Similarly, LLDP data received through trunked ports is stored individually, per-port.

**IP Address Advertisements.** In the default operation, if a port belongs to only one static VLAN, then the port advertises the lowest-order IP address configured on that VLAN. If a port belongs to multiple VLANs, then the port advertises the lowest-order IP address configured on the VLAN with the lowest VID. If the qualifying VLAN does not have an IP address, the port advertises 127.0.0.1 as its IP address. For example, if the port is a member of the default VLAN (VID = 1), and there is an IP address configured for the default VLAN, then the port advertises this IP address. In the default operation, the IP address that LLDP uses can be an address acquired by DHCP or Bootp.

You can override the default operation by configuring the port to advertise any IP address that is manually configured on the switch, even if the port does not belong to the VLAN configured with the selected IP address (page 5-47). (Note that LLDP cannot be configured through the CLI to advertise an addresses acquired through DHCP or Bootp. However, as mentioned above, in the default LLDP configuration, if the lowest-order IP address on the VLAN with the lowest VID for a given port is a DHCP or Bootp address, then the switch includes this address in its LLDP advertisements unless another address is configured for advertisements on that port.) Also, although LLDP allows configuring multiple remote management addresses on a port, only the lowest-order address configured on the port will be included in outbound advertisements. Attempting to use the CLI to configure LLDP with an IP address that is either not configured on a VLAN, or has been acquired by DHCP or Bootp results in the following error message.

```
xxx.xxx.xxx.xxx: This IP address is not configured or is
a DHCP address.
```

**Spanning-Tree Blocking.** Spanning tree does not prevent LLDP packet transmission or receipt on STP-blocked links.

**802.1X Blocking.** Ports blocked by 802.1X operation do not allow transmission or receipt of LLDP packets.

# Configuring LLDP Operation

In the default configuration, LLDP is enabled and in both transmit and receive mode on all active ports. The LLDP configuration includes global settings that apply to all active ports on the switch, and per-port settings that affect only the operation of the specified ports.

The commands in this section affect both LLDP and LLDP-MED operation. for information on operation and configuration unique to LLDP-MED, refer to "LLDP-MED (Media-Endpoint-Discovery)" on page 5-50.


| Command | Page |
|---|---|
| show lldp config | 5-42 |
| [no] lldp run | 5-42 |
| lldp refresh-interval | 5-43 |
| lldp holdtime-multiplier | 5-43 |
| lldpTxDelay | 5-44 |
| lldpReinitDelay | 5-45 |
| lldp enable-notification | 5-45 |
| lldpnotificationinterval | 5-46 |
| lldp admin-status < txonly \| rxonly \| tx_rx \| disable > | 5-46 |
| lldp config < *port-list* > IpAddrEnable | 5-47 |
| lldp config < *port-list* > basicTlvEnable | 5-48 |
| lldp config < *port-list* > dot3TlvEnable < macphy_config > | 5-49 |


## Viewing the Current Configuration

**Displaying the Global LLDP, Port Admin, and SNMP Notification Status.** This command displays the switch's general LLDP configuration status, including some per-port information affecting advertisement traffic and trap notifications.

***Syntax*** show lldp config

Displays the LLDP global configuration, LLDP port status, and SNMP notification status. For information on port admin status, refer to "Configuring Per-Port Transmit and Receive Modes" on page 5-46.

For example, **show lldp config** produces the following display when the switch is in the default LLDP configuration:

```
HP Switch(config)# show lldp config

 LLDP Global Configuation

  LLDP Enabled [Yes] : Yes
  LLDP Transmit Interval    [30] : 30
  LLDP Hold time Multiplier  [4] : 4
  LLDP Delay Interval        [2] : 2
  LLDP Reinit Interval       [2] : 2
  LLDP Notification Interval [5] : 5
  LLDP Fast Start Count      [5] : 5

 LLDP Port Configuration
  Port  | AdminStatus NotificationEnabled Med Topology Trap Enabled
  ----- + ----------- ------------------- -------------------------
  1     | Tx_Rx       False               False
  2     | Tx_Rx       False               False
  3     | Tx_Rx       False               False
  4     | Tx_Rx       False               False
  5     | Tx_Rx       False               False
```

**Note:** This value corresponds to the lldp refresh-interval command (page 5-43).

**Figure 5-17. Example of Viewing the General LLDP Configuration**

**Displaying Port Configuration Details.** This command displays the port-specific configuration, including.

***Syntax*** show lldp config < *port-list* >

*Displays the LLDP port-specific configuration for all ports in* < *port-list*>, *including which optional TLVs and any non-default IP address that are included in the port's outbound advertisements. For information on the notification setting, refer to "Configuring SNMP Notification Support" on page 5-45. For information on the other configurable settings displayed by this command, refer to "Configuring Per-Port Transmit and Receive Modes" on page 5-46.*

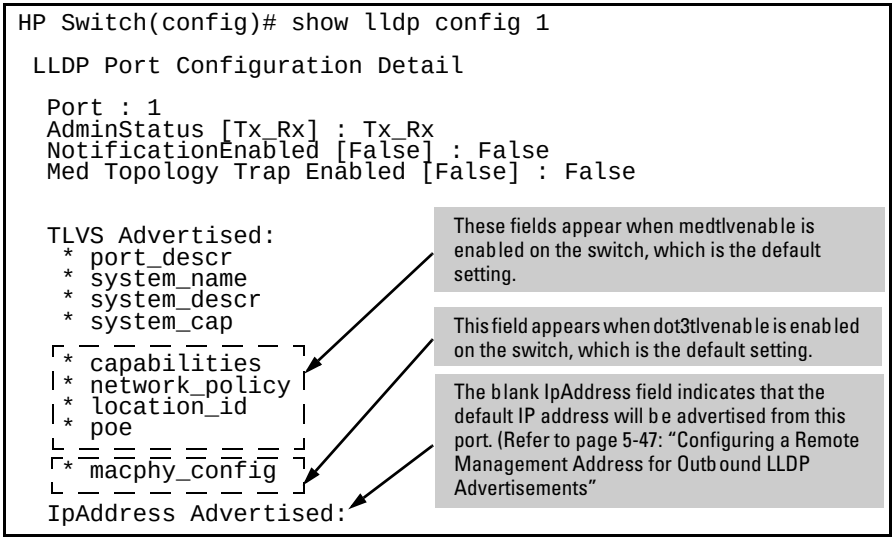



**Figure 5-18. Example of Per-Port Configuration Display**

## Configuring Global LLDP Packet Controls

The commands in this section configure the aspects of LLDP operation that apply the same to all ports in the switch.

**Enabling or Disabling LLDP Operation on the Switch.** Enabling LLDP operation (the default) causes the switch to:

- Use active, LLDP-enabled ports to transmit LLDP packets describing itself to neighbor devices.
- Add entries to its neighbors table based on data read from incoming LLDP advertisements.

***Syntax*** [ no ] lldp run

*Enables or disables LLDP operation on the switch. The* **no** *form of the command, regardless of individual LLDP port configurations, prevents the switch from transmitting outbound LLDP advertisements, and causes the switch to drop all LLDP advertisements received from other devices. The switch preserves the current LLDP configuration when LLDP is disabled. After LLDP is disabled, the information in the LLDP neighbors database remains until it times-out. (Default: Enabled)*

For example, to disable LLDP on the switch:

```
HP Switch(config)# no lldp run
```

**Changing the Packet Transmission Interval.** This interval controls how often active ports retransmit advertisements to their neighbors.

***Syntax*** lldp refresh-interval < 5 - 32768 >

*Changes the interval between consecutive transmissions of LLDP advertisements on any given port. (Default: 30 seconds)*

**Note:** *The* **refresh-interval** *must be greater than or equal to (4 x* **delay-interval***). (The default* **delay-interval** *is 2). For example, with the default* **delay-interval**, *the lowest* **refresh-interval** *you can use is 8 seconds (4 x 2 = 8). Thus, if you want a* **refresh-interval** *of 5 seconds, you must first change the delay interval to 1 (that is, 4 x 1 < 5). If you want to change the* **delay-interval**, *use the* **setmib** *command.*

**Changing the Time-to-Live for Transmitted Advertisements.** The Time-to-Live value (in seconds) for all LLDP advertisements transmitted from a switch is controlled by the switch that generates the advertisement, and determines how long an LLDP neighbor retains the advertised data before discarding it. The Time-to-Live value is the result of multiplying the **refresh-interval** by the **holdtime-multiplier** described below.

***Syntax*** lldp holdtime-multiplier < 2 - 10 >

*Changes the multiplier an LLDP switch uses to calculate the Time-to-Live for the LLDP advertisements it generates and transmits to LLDP neighbors. When the Time-to-Live for a given advertisement expires the advertised data is deleted from the neighbor switch's MIB. (Default: 4; Range: 2 - 10)*

For example, if the refresh-interval on the switch is 15 seconds and the **holdtime-multiplier** is at the default, the Time-to-Live for advertisements transmitted from the switch is 60 seconds (4 x 15). To reduce the Time-to-Live, you could lower the **holdtime-interval** to 2, which would result in a Time-to-Live of 30 seconds.

```
HP Switch(config)# lldp holdtime-multiplier 2
```

**Changing the Delay Interval Between Advertisements Generated by Value or Status Changes to the LLDP MIB.** The switch uses a *delay-interval* setting to delay transmitting successive advertisements resulting from these LLDP MIB changes. If a switch is subject to frequent changes to its LLDP MIB, lengthening this interval can reduce the frequency of successive advertisements. The delay-interval can be changed using either an SNMP network management application or the CLI **setmib** command.

***Syntax*** setmib lldpTxDelay.0 -i < 1 - 8192 >

*Uses* **setmib** *to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. (Default: 2; Range: 1 - 8192)*

**Note:** *The LLDP refresh-interval (transmit interval) must be greater than or equal to (4 x delay-interval). The switch does not allow increasing the delay interval to a value that conflicts with this relationship. That is, the switch displays* **Inconsistent value** *if (4 x delay-interval) exceeds the current transmit interval, and the command fails. Depending on the current refresh-interval setting, it may be necessary to increase the refresh-interval before using this command to increase the delay-interval.*

For example, to change the delay-interval from 2 seconds to 8 seconds when the refresh-interval is at the default 30 seconds, you must first set the refresh-interval to a minimum of 32 seconds (32 = 4 x 8).

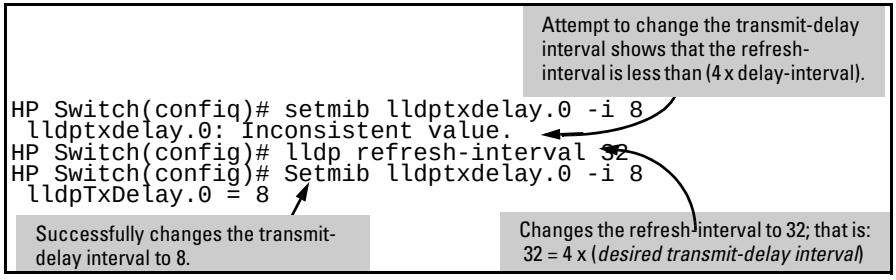



**Figure 5-19. Example of Changing the Transmit-Delay Interval**

**Changing the Reinitialization Delay Interval.** In the default configuration, a port receiving a **disable** command followed immediately by a **txonly**, **rxonly**, or **tx_rx** command delays reinitializing for two seconds, during which time LLDP operation remains disabled. If an active port is subjected to frequent toggling between the LLDP disabled and enabled states, LLDP advertisements are more frequently transmitted to the neighbor device. Also, the neighbor table in the adjacent device will change more frequently, as it deletes, then replaces LLDP data for the affected port which, in turn, generates SNMP traps (if trap receivers and SNMP notification are configured). All of this can unnecessarily increase network traffic. Extending the reinitialization-delay interval delays the port's ability to reinitialize and generate LLDP traffic following an LLDP disable/enable cycle.

***Syntax*** setmib lldpReinitDelay.0 -i < 1 - 10 >

*Uses* **setmib** *to change the minimum time (reinitialization delay interval) an LLDP port will wait before reinitializing after receiving an LLDP disable command followed closely by a txonly or tx_rx command. The delay interval commences with execution of the* **lldp admin-status < port-list > disable** *command. (Default: 2 seconds; Range: 1 - 10 seconds)*

For example, the following command changes the reinitialization delay interval to five seconds:

```
HP Switch(config)# setmib lldpreinitdelay.0 -i 5
```

## Configuring SNMP Notification Support

You can enable SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices, and control the interval between successive notifications of data changes on the same neighbor.

**Enabling LLDP Data Change Notification for SNMP Trap Receivers.**

***Syntax*** [ no ] lldp enable-notification < *port-list* >

*Enables or disables each port in < port-list > for sending notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. (**Default**: Disabled)*
*For information on configuring trap receivers in the switch, refer to "SNMP Notifications" on page 5-14.*

For example, this command enables SNMP notification on ports 1 - 5:

```
HP Switch(config)# lldp enable-notification 1-5
```

**Changing the Minimum Interval for Successive Data Change Notifications for the Same Neighbor.**

If LLDP trap notification is enabled on a port, a rapid succession of changes in LLDP information received in advertisements from one or more neighbors can generate a high number of traps. To reduce this effect, you can globally change the interval between successive notifications of neighbor data change.

***Syntax*** setmib lldpnotificationinterval.0 -i < 1 - 3600 >

*Globally changes the interval between successive traps generated by the switch. If multiple traps are generated in the specified interval, only the first trap will be sent. The remaining traps will be suppressed. (A network management application can periodically check the switch MIB to detect any missed change notification traps. Refer to IEEE P802.1AB or later for more information.) (Default: 5 seconds)*

For example, the following command limits change notification traps from a particular switch to one per minute.

```
HP Switch(config)# setmib lldpnotificationinterval.0 -i
60
lldpNotificationInterval.0 = 60
```

## Configuring Per-Port Transmit and Receive Modes

These commands control advertisement traffic inbound and outbound on active ports.

***Syntax*** lldp admin-status < *port-list* > < txonly | rxonly | tx_rx | disable >

*With LLDP enabled on the switch in the default configuration, each port is configured to transmit and receive LLDP packets. These options enable you to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.*

**txonly**: *Configures the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.*

**rxonly**: *Configures the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors.*

**tx_rx**: *Configures the specified port(s) to both transmit and receive LLDP packets. (This is the default setting.)*

**disable**: *Disables LLDP packet transmit and receive on the specified port(s).*

## Configuring Basic LLDP Per-Port Advertisement Content

In the default LLDP configuration, outbound advertisements from each port on the switch include both mandatory and optional data.

**Mandatory Data.** An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. LLDP collects the mandatory data, and, except for the Remote Management Address, you cannot use LLDP commands to configure the actual data.

- Chassis Type (TLV subelement)
- Chassis ID (TLV)
- Port Type (TLV subelement)
- Port ID (TLV)
- Remote Management Address (TLV; actual IP address is a subelement that can be a default address or a configured address)

**Configuring a Remote Management Address for Outbound LLDP Advertisements.** This is an optional command you can use to include a specific IP address in the outbound LLDP advertisements for specific ports.

***Syntax*** [ no ] lldp config < *port-list* > ipAddrEnable < *ip-address* >

*Replaces the default IP address for the port with an IP address you specify. This can be any IP address configured in a static VLAN on the switch, even if the port does not belong to the VLAN configured with the selected IP address. The* **no** *form of the command deletes the specified IP address. If there are no IP addresses configured as management addresses, then the IP address selection method returns to the default operation. (Default: The port advertises the IP address of the lowest-numbered VLAN (VID) to which it belongs. If there is no IP address configured on the VLAN(s) to which the port belongs, and the port is not configured to advertise an IP address from any other (static) VLAN on the switch, then the port advertises an address of 127.0.0.1.)*

**Note:** *This command does not accept either IP addresses acquired through DHCP or Bootp, or IP addresses that are not configured in a static VLAN on the switch*

For example, if port 3 belongs to a subnetted VLAN that includes an IP address of 10.10.10.100 and you wanted port 3 to use this secondary address in LLDP advertisements, you would need to execute the following command:

```
HP Switch(config)# lldp config 3 ipAddrEnable
10.10.10.100
```

**Optional Data.** You can configure an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. Note that optional data types, when enabled, are populated with data internal to the switch; that is, you cannot use LLDP commands to configure their actual content.

- port description (TLV)
- system name (TLV)
- system description (TLV)
- system capabilities (TLV)
  - system capabilities Supported (TLV subelement)
  - system capabilities Enabled (TLV subelement)
- port speed and duplex (TLV subelement)

***Syntax:*** [ no ] lldp config < *port-list* > basicTlvEnable < *TLV-Type* >

port_descr

*For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the port.*
*(Default: Enabled)*

system_name

*For outbound LLDP advertisements, this TLV includes an alphanumeric string showing the system's assigned name.*
*(Default: Enabled)*

system_descr

*For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.*
*(Default: Enabled)*

system_cap

*For outbound advertisements, this TLV includes a bitmask of supported system capabilities (device functions). Also includes information on whether the capabilities are enabled.*
*(Default: Enabled)*

For example, if you wanted to exclude the system name TLV from the outbound LLDP advertisements for all ports on a switch, you would use this command:

```
HP Switch(config)# no lldp config 1-24 basicTlvEnable
system_name
```

If you later decided to reinstate the system name TLV on ports 1-5, you would use this command:

```
HP Switch(config)# lldp config 1-5 basicTlvEnable
system_name
```

## Configuring Support for Port Speed and Duplex Advertisements

This feature is optional for LLDP operation, but is *required* for LLDP-MED operation.

Port speed and duplex advertisements are supported on the switches covered in this guide to inform an LLDP endpoint and the switch port of each other's port speed and duplex configuration and capabilities. Configuration mismatches between a switch port and an LLDP endpoint can result in excessive collisions and voice quality degradation. LLDP enables discovery of such mismatches by supporting SNMP access to the switch MIB for comparing the current switch port and endpoint settings. (Changing a current device configuration to eliminate a mismatch requires intervention by the system operator.)

***Syntax:*** [ no ] lldp config < *port-list* > dot3TlvEnable macphy_config

*For outbound advertisements, this TLV includes the (local) switch port's current speed and duplex settings, the range of speed and duplex settings the port supports, and the method required for reconfiguring the speed and duplex settings on the device (auto-negotiation during link initialization, or manual configuration).*

*Using SNMP to compare local and remote information can help in locating configuration mismatches.*

*(Default: Enabled)*

***Note:*** *For LLDP operation, this TLV is optional. For LLDP-MED operation, this TLV is mandatory.*

As mentioned above, an SNMP network management application can be used to compare the port speed and duplex data configured in the switch and advertised by the LLDP endpoint. You can also use the CLI to display this

information. For more on using the CLI to display port speed and duplex information, refer to “Displaying the Current Port Speed and Duplex Configuration on a Switch Port” on page 5-64.

## LLDP-MED (Media-Endpoint-Discovery)

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to LLDP-MED operation. The **show** commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED benefits include:

- plug-and-play provisioning for MED-capable, VoIP endpoint devices
- simplified, vendor-independent management enabling different IP telephony systems to interoperate on one network
- automatic deployment of convergence network policies (voice VLANs, Layer 2/CoS priority, and Layer 3/QoS priority)
- configurable endpoint location data to support the Emergency Call Service (ECS) (such as Enhanced 911 service, 999, 112)
- detailed VoIP endpoint data inventory readable via SNMP from the switch
- Power over Ethernet (PoE) status and troubleshooting support via SNMP
- support for IP telephony network troubleshooting of call quality issues via SNMP

This section describes how to configure and use LLDP-MED features in the switches to support VoIP network edge devices (Media Endpoint Devices) such as:

- IP phones
- voice/media gateways
- media servers
- IP communications controllers
- other VoIP devices or servers

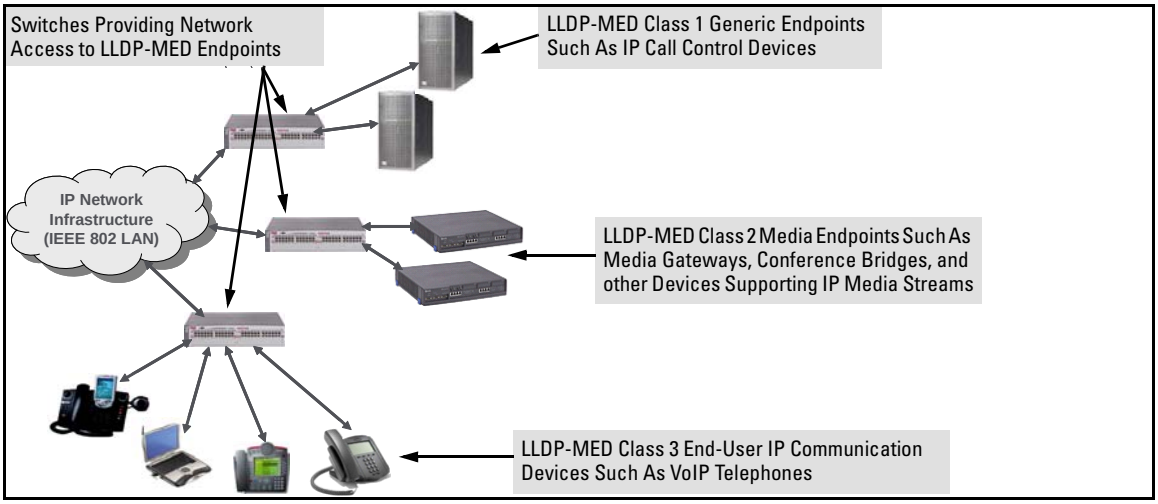



**Figure 5-20. Example of LLDP-MED Network Elements**

**LLDP-MED Endpoint Support.** LLDP-MED on the switches covered in this guide interoperates with directly connected IP telephony (endpoint) clients having these features and services:

- able to autonegotiate speed and duplex configuration with the switch
- able to use the following network policy elements configured on the client port
  - voice VLAN ID
  - 802.1p (Layer 2) QoS
  - Diffserv codepoint (DSCP) (Layer 3) QoS
- discover and advertise device location data learned from the switch
- support emergency call service (ECS—such as E911, 999, and 112)
- advertise device information for the device data inventory collected by the switch, including:
  - hardware revision
  - firmware revision
  - software revision
  - serial number
  - manufacturer name
  - model name
  - asset ID
- provide information on network connectivity capabilities (for example, a multi-port VoIP phone with Layer 2 switch capability)
- support the fast start capability

**Note** LLDP-MED on the switches covered in this guide is intended for use with VoIP endpoints, and is not designed to support links between network infrastructure devices, such as switch-to-switch or switch-to-router links.

**LLDP-MED Endpoint Device Classes.** LLDP-MED endpoint devices are, by definition, located at the network edge and communicate using the LLDP-MED framework. Any LLDP-MED endpoint device belongs to one of the following three classes:

- Class 1 (Generic Endpoint Devices): These devices offer the basic LLDP discovery services, network policy advertisement (VLAN ID, Layer 2/802.1p priority, and Layer 3/DSCP priority), and PoE management. This class includes such devices as IP call controllers and communication-related servers.
- Class 2 (Media Endpoint Devices): These devices offer all Class 1 features plus media streaming capability, and include such devices as voice/media gateways, conference bridges, and media servers.
- Class 3 (Communication Devices): These devices are typically IP phones or end-user devices that otherwise support IP media and offer all Class 1 and Class 2 features, plus location identification and emergency 911 capability, Layer 2 switch support, and device information management.

**LLDP-MED Operational Support.** The switches covered in this guide offer two configurable TLVs supporting MED-specific capabilities:

- medTlvEnable (for per-port enabling or disabling of LLDP-MED operation)
- medPortLocation (for configuring per-port location or emergency call data)

**Note** LLDP-MED operation also requires the port speed and duplex TLV (dot3TlvEnable; page 5-49), which is enabled in the default configuration.

## LLDP-MED Topology Change Notification

This optional feature provides information an SNMP application can use to track LLDP-MED connects and disconnects.

***Syntax:*** lldp top-change-notify < *port-list* >

*Topology change notification, when enabled on an LLDP port, causes the switch to send an SNMP trap if it detects LLDP-MED endpoint connection or disconnection activity on the port, or an age-out of the LLDP-MED neighbor on the port. The trap includes the following information*:

- *the port number (internal) on which the activity was detected (For more in internal port numbers, refer to "Determining the Switch Port Number Included in Topology Change Notification Traps" on page 5-70.)*
- *the LLDP-MED class of the device detected on the port ("LLDP-MED Endpoint Device Classes" on page 5-52.)*

*The* **show running** *command shows whether the topology change notification feature is enabled or disabled. For example, if ports 1-10 have topology change notification enabled, the following entry appears in the* **show running** *output:*

```
lldp top-change-notify 1-10
```

*(Default: Disabled)*

***Note:*** *To send traps, this feature requires access to at least one SNMP server. For information on configuring traps, refer to "SNMP Notifications" on page 5-14.*

*Also, if a detected LLDP-MED neighbor begins sending advertisements without LLDP-MED TLVs, the switch sends a top-change-notify trap.*

**Note**

Topology change notifications provide one method for monitoring system activity. However, because SNMP normally employs UDP, which does not guarantee datagram delivery, topology change notification should not be relied upon as the sole method for monitoring critical endpoint device connectivity.

## LLDP-MED Fast Start Control

***Syntax:*** lldp fast-start-count < 1 - 10 >

*An LLDP-MED device connecting to a switch port may use the data contained in the MED TLVs from the switch to configure itself. However, the* **lldp refresh-interval** *setting (default: 30 seconds) for transmitting advertisements can cause an unacceptable delay in MED device configuration. To support rapid LLDP-MED device configuration, the* **lldp fast-start-count** *command temporarily overrides the* **refresh-interval** *setting for the* **fast-start-count** *advertisement interval. This results in the port initially advertising LLDP-MED at a faster rate for a limited time. Thus, when the switch detects a new LLDP-MED device on a port, it transmits one LLDP-MED advertisement per second out the port for the duration of the* **fast-start-count** *interval. In most cases, the default setting should provide an adequate* **fast-start-count** *interval.*

*(Range:* **1 - 10** *seconds; Default:* **5** *seconds)*

**Note:** *This global command applies only to ports on which a new LLDP-MED device is detected. It does not override the refresh-interval setting on ports where non-MED devices are detected.*

## Advertising Device Capability, Network Policy, PoE Status and Location Data

The medTlvEnable option on the switch is enabled in the default configuration and supports the following LLDP-MED TLVs:

- LLDP-MED capabilities: This TLV enables the switch to determine:
  - whether a connected endpoint device supports LLDP-MED
  - which specific LLDP-MED TLVs the endpoint supports
  - the device class (1, 2, or 3) for the connected endpoint

  This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.
- network policy operating on the port to which the endpoint is connected (VLAN, Layer 2 QoS, Layer 3 QoS)
- PoE (MED Power-over-Ethernet)
- physical location data — page 5-58

**Note**

LLDP-MED operation requires the macphy_config TLV subelement—enabled by default—that is optional for IEEE 802.1AB LLDP operation. Refer to the **dot3TlvEnable macphy_config** command on page 5-49.

**Network Policy Advertisements.** Network policy advertisements are intended for real-time voice and video applications, and include these TLV subelements:

- Layer 2 (802.1p) QoS
- Layer 3 DSCP (diffserv code point) QoS
- Voice VLAN ID (VID)

**VLAN Operating Rules.** These rules affect advertisements of VLANs in network policy TLVs:

- The VLAN ID TLV subelement applies only to a VLAN configured for voice operation (**vlan *< vid >* voice**).
- If there are multiple voice VLANs configured on a port, LLDP-MED advertises the voice VLAN having the lowest VID.
- The voice VLAN port membership configured on the switch can be tagged or untagged. However, if the LLDP-MED endpoint expects a tagged membership when the switch port is configured for untagged, or the reverse, then a configuration mismatch results. (Typically, the endpoint expects the switch port to have a tagged voice VLAN membership.)
- If a given port does not belong to a voice VLAN, then the switch does not advertise the VLAN ID TLV through this port.

**Policy Elements.** These policy elements may be statically configured on the switch or dynamically imposed during an authenticated session on the switch using a RADIUS server and 802.1X or MAC authentication. (Web authentication does not apply to VoIP telephones and other telecommunications devices that are not capable of accessing the switch through a Web browser.) The QoS and voice VLAN policy elements can be statically configured with the following CLI commands:

vlan < *vid* > voice

vlan < *vid* > < tagged | untagged > < *port-list* >

int < *port-list* > qos priority < 0 - 7 >

vlan < *vid* > qos dscp < *codepoint* >

**Notes**

A codepoint must have an 802.1p priority before you can configure it for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows **No Override** in the **Priority** column of the DSCP policy table (display with **show qos-dscp map**, then use **qos-dscp map < *codepoint* > priority < 0 - 7 >** to configure a priority before proceeding. For more on this topic, refer to the chapter titled "Quality of Service (QoS): Managing Bandwidth More Effectively" in the *Advanced Traffic Management Guide* for your switch.

**Enabling or Disabling medTlvEnable.** In the default LLDP-MED configuration, the TLVs controlled by medTlvEnable are enabled.

***Syntax:*** [ no ] lldp config < *port-list* > medTlvEnable < *medTlv* >

- *Enables or disables advertisement of the following TLVs on the specified ports:*
  - *device capability TLV*
  - *configured network policy TLV*
  - *configured location data TLV (Refer to "Configuring Location Data for LLDP-MED Devices" on page 5-58.)*
  - *current PoE status TLV*

  *(Default: All of the above TLVs are enabled.)*
- *Helps to locate configuration mismatches by allowing use of an SNMP application to compare the LLDP-MED configuration on a port with the LLDP-MED TLVs advertised by a neighbor connected to that port.*

capabilities

This TLV enables the switch to determine:

- *which LLDP-MED TLVs a connected endpoint can discover*
- *the device class (1, 2, or 3) for the connected endpoint*

*This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.*

*(Default: enabled)*

**Note:** This TLV cannot be disabled unless the network_policy, poe, and location_id TLVs are already disabled.

network-policy

*This TLV enables the switch port to advertise its configured network policies (voice VLAN, Layer 2 QoS, Layer 3 QoS), and allows LLDP-MED endpoint devices to auto-configure the voice network policy advertised by the switch. This also enables the use of SNMP applications to troubleshoot statically configured endpoint network policy mismatches.*

*(Default: Enabled)*

***Notes:*** *Network policy is only advertised for ports that are configured as members of the voice VLAN. If the port belongs to more than one voice VLAN, then the voice VLAN with the lowest-numbered VID is selected as the VLAN for voice traffic. Also, this TLV cannot be enabled unless the* capability *TLV is already enabled.*

*For more information, refer to "Network Policy Advertisements" on page 5-55*

location_id

*This TLV enables the switch port to advertise its configured location data (if any). For more on configuring location data, refer to "Configuring Location Data for LLDP-MED Devices".*

*(Default: Enabled)*

***Note:*** *When disabled, this TLV cannot be enabled unless the* capability *TLV is already enabled.*

poe

*This TLV enables the switch port to advertise its current PoE (Power over Ethernet) state and to read the PoE requirements advertised by the LLDP-MED endpoint device connected to the port.*

*(Default: Enabled)*

***Note:*** *When disabled, this TLV cannot be enabled unless the* capability *TLV is already enabled.*

For more on this topic, refer to "PoE Advertisements", below.

**PoE Advertisements.** These advertisements inform an LLDP-MED endpoint of the power (PoE) configuration on switch ports. Similar advertisements from an LLDP-MED endpoint inform the switch of the endpoint's power needs and provide information that can be used to identify power priority mismatches.

Power-over-Ethernet TLVs include the following power data:

- **power type:** indicates whether the device is a power-sourcing entity (PSE) or a powered device (PD). A MED-capable VoIP telephone is a PD.
- **power source**: indicates the source of power in use by the device. Power sources for powered devices (PDs) include PSE, local (internal), and PSE/local. The switches covered in this guide advertise Unknown.
- **power priority:** indicates the power priority configured on the switch (PSE) port or the power priority configured on the MED-capable endpoint.
- **power value:** indicates the total power in watts that a switch port (PSE) can deliver at a particular time, or the total power in watts that the MED endpoint (PD) requires to operate.

To display the current power data for an LLDP-MED device connected to a port, use the following command:

**show lldp info remote-device < port-list >**

For more on this command, refer to page 5-65.

To display the current PoE configuration on the switch, use the following commands:

**show power brief < port-list >**

**show power < port-list >**

For more on PoE configuration and operation, refer to Chapter , "Power Over Ethernet (PoE/PoE+) Operation".

## Configuring Location Data for LLDP-MED Devices

You can configure a switch port to advertise location data for the switch itself, the physical wall-jack location of the endpoint (recommended), or the location of a DHCP server supporting the switch and/or endpoint. You also have the option of configuring these different address types:

- **civic address:** physical address data such as city, street number, and building information

- **ELIN (Emergency Location Identification Number):** an emergency number typically assigned to MLTS (Multiline Telephone System Operators) in North America
- **coordinate-based location:** attitude, longitude, and altitude information (Requires configuration via an SNMP application.)

***Syntax:*** [ no ] lldp config < *port-list* > medPortLocation < *Address-Type* >

*Configures location or emergency call data the switch advertises per port in the* **location_id** *TLV. This TLV is for use by LLDP-MED endpoints employing location-based applications.*

***Note:*** *The switch allows one medPortLocation entry per port (without regard to type). Configuring a new medPortLocation entry of any type on a port replaces any previously configured entry on that port.*

civic-addr < *COUNTRY-STR* > < *WHAT* > < *CA-TYPE* > < *CA-VALUE* > . . . [< *CA-TYPE* > < *CA-VALUE* >] . . . [< *CA-TYPE* > < *CA-VALUE* >]

*This command enables configuration of a physical address on a switch port, and allows up to 75 characters of address information.*

**COUNTRY-STR:** *A two-character country code, as defined by ISO 3166. Some examples include* **FR** *(France),* **DE** *(Germany), and* **IN** *(India). This field is required in a* **civic-addr** *command. (For a complete list of country codes, visit* **www.iso.org** *on the world wide web.)*

**WHAT:** *A single-digit number specifying the type of device to which the location data applies:*

- **0:** *Location of DHCP server*
- **1:** *Location of switch*
- **2:** *Location of LLDP-MED endpoint (recommended application)*

*This field is required in a* **civic-addr** *command.*

*—Continued—*

*— Continued—*

***Type/Value Pairs (*CA-TYPE *and* CA-VALUE*):*** *This is a series of data pairs, each composed of a location data "type" specifier and the corresponding location data for that type. That is, the first value in a pair is expected to be the civic address "type" number (**CA-TYPE**), and the second value in a pair is expected to be the corresponding civic address data (**CA-VALUE**). For example, if the **CA-TYPE** for "city name" is "**3**", then the type/value pair to define the city of Paris is "**3 Paris**". Multiple type/value pairs can be entered in any order, although it is recommended that multiple pairs be entered in ascending order of the **CA-TYPE**. When an emergency call is placed from a properly configured class 3 endpoint device to an appropriate PSAP, the country code, device type, and type/value pairs configured on the switch port are included in the transmission. The "type" specifiers are used by the PSAP to identify and organize the location data components in an understandable format for response personnel to interpret. A* **civic-addr** *command requires a minimum of one type/value pair, but typically includes multiple type/value pairs as needed to configure a complete set of data describing a given location.* ***CA-TYPE****: This is the first entry in a type/value pair, and is a number defining the type of data contained in the second entry in the type/value pair (**CA-VALUE**). Some examples of **CA-TYPE** specifiers include:*

- *3 = city*
- *6 = street (name)*
- *25 = building name*

*(Range: 0 - 255)*

*For a sample listing of **CA-TYPE** specifiers, refer to table 5-4 on page 5-61.*

***CA-VALUE****: This is the second entry in a type/value pair, and is an alphanumeric string containing the location information corresponding to the immediately preceding **CA-TYPE** entry. Strings are delimited by either blank spaces, single quotes ('... '), or double quotes ("... "). Each string should represent a specific data type in a set of unique type/value pairs comprising the description of a location, and each string must be preceded by a **CA-TYPE** number identifying the type of data in the string.*

***Note:*** *A switch port allows one instance of any given* ***CA-TYPE****. For example, if a type/value pair of* **6 Atlantic** *(to specify "Atlantic" as a street name) is configured on port 5 and later another type/value pair of* **6 Pacific** *is configured on the same port, then* **Pacific** *replaces* **Atlantic** *in the civic address location configured for port 5.*

elin-addr < *emergency-number* >

*This feature is intended for use in Emergency Call Service (ECS) applications to support class 3 LLDP-MED VoIP telephones connected to a switch covered in this guide in a multiline telephone system (MLTS) infrastructure. An ELIN (Emergency Location Identification Number) is a valid North American Numbering Plan (NANP) format telephone number assigned to MLTS operators in North America by the appropriate authority. The ELIN is used to route emergency (E911) calls to a Public Safety Answering Point (PSAP).*

*(Range: 1-15 numeric characters)*

**Configuring Coordinate-Based Locations.** Latitude, longitude, and altitude data can be configured per switch port using an SNMP management application. For more information, refer to the documentation provided with the application. A further source of information on this topic is *RFC 3825-Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information.*

**Note**

Endpoint use of data from a medPortLocation TLV sent by the switch is device-dependent. Refer to the documentation provided with the endpoint device.

**Table 5-4. Some Location Codes Used in CA-TYPE Fields***

| Location Element | Code | Location Element | Code |
|---|---|---|---|
| national subdivision | 1 | street number | 19 |
| regional subdivision | 2 | additional location data | 22 |
| city or township | 3 | unit or apartment | 26 |
| city subdivision | 4 | floor | 27 |
| street | 6 | room number | 28 |
| street suffix | 18 | | |

*The code assignments in this table are examples from a work-in-progress (the internet draft titled "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information draft-ietf-geopriv-dhcp-civil-06" dated May 30, 2005.) For the actual codes to use, contact the PSAP or other authority responsible for specifying the civic addressing data standard for your network.

**Example of a Location Configuration.** Suppose a system operator wanted to configure the following information as the civic address for a telephone connected to her company's network through port 2 of a switch at the following location:

| Description | CA-Type | CA-VALUE |
|---|---|---|
| national subdivision | 1 | CA |
| city | 3 | Widgitville |
| street | 6 | Main |
| street number | 19 | 1433 |
| unit | 26 | Suite 4-N |
| floor | 27 | 4 |
| room number | 28 | N4-3 |

Figure 5-21 shows the commands for configuring and displaying the above data.

```
HP Switch(config)# lldp config 2 medportlocation civic-addr US 2 1 CA 3 Widgit-
ville 6 Main 19 1433 26 Suite_4-N 27 4 28 N4-3

HP Switch(config)# show lldp config 2

 LLDP Port Configuration Detail

  Port : 2
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False

  Country Name                : US
  What                        : 2
  Ca-Type                     : 1
  Ca-Length                   : 2
  Ca-Value                    : CA
  Ca-Type                     : 3
  Ca-Length                   : 11
  Ca-Value                    : Widgitville
  Ca-Type                     : 6
  Ca-Length                   : 4
  Ca-Value                    : Main
  Ca-Type                     : 19
  Ca-Length                   : 4
  Ca-Value                    : 1433
  Ca-Type                     : 26
  Ca-Length                   : 9
  Ca-Value                    : Suite_4-N
  Ca-Type                     : 27
  Ca-Length                   : 1
  Ca-Value                    : 4
  Ca-Type                     : 28
  Ca-Length                   : 4
  Ca-Value                    : N4-3
```

**Figure 5-21. Example of a Civic Address Configuration**

# Displaying Advertisement Data

| Command | Page |
|---|---|
| show lldp info local-device | below |
| walkmib lldpXdot3LocPortOperMauType | |
| show lldp info remote-device | 5-65 |
| walkmib lldpXdot3RemPortAutoNegAdvertisedCap | |
| show lldp info stats | 5-67 |

## Displaying Switch Information Available for Outbound Advertisements

These commands display the current switch information that will be used to populate outbound LLDP advertisements.

***Syntax*** show lldp info local-device [ *port-list* ]

*Without the [ port-list ] option, this command displays the global switch information and the per-port information currently available for populating outbound LLDP advertisements.*

*With the* [ port-list ] *option, this command displays only the following port-specific information that is currently available for outbound LLDP advertisements on the specified ports:*

- **PortType**
- **PortId**
- **PortDesc**

**Note:** *This command displays the information available on the switch. Use the* **lldp config < port-list >** *command to change the selection of information that is included in actual outbound advertisements. In the default LLDP configuration, all information displayed by this command is transmitted in outbound advertisements.*

For example, in the default configuration, the switch information currently available for outbound LLDP advertisements appears similar to the display in Figure 5-22 on page 5-64.

```
HP Switch(config)# show lldp info local-device

 LLDP Local Device Information

  Chassis Type : mac-address
  Chassis Id   : 00 23 47 4b 68 00
  System Name  : HP-2520G-24-PoE
  System Description : HP J9299A Switch 2520G-24-PoE, revision YA.15.XX...
  System Capabilities Supported:bridge
  System Capabilities Enabled:bridge

 Management Address  :
    Type:ipv4
    Address:

 LLDP Port Information

  Port     | PortType PortId   PortDesc
  -------- + -------- -------- --------
  1        | local    1        1
  2        | local    2        2
  3        | local    3        3
  4        | local    4        4
  5        | local    5        5
  6        | local    6        6
  .          .        .        .
```

The Management Address field displays only the LLDP-configurable IP addresses on the switch. (Only manually-configured IP addresses are LLDP-configurable.) If the switch has only an IP address from a DHCP or Bootp server, then the Management Address field is empty (because there are no LLDP-configurable IP addresses available). For more on this topic, refer to "Remote Management Address" on page 5-38.

**Figure 5-22. Example of Displaying the Global and Per-Port Information Available for Outbound Advertisements**

```
HP Switch(config)# show lldp info local 1-
2

 LLDP Local Port Information Detail

  Port     : 1
  PortType : local
  PortId   : 1
  PortDesc : 1

----------------------------------------
  Port     : 2
  PortType : local
  PortId   : 2
  PortDesc : 2
```

**Figure 5-23. Example of the Default Per-Port Information Content for Ports 1 and 2**

**Displaying the Current Port Speed and Duplex Configuration on a Switch Port.** Port speed and duplex information for a switch port and a connected LLDP-MED endpoint can be compared for configuration mismatches by using an SNMP application. You can also use the switch CLI to display this information, if necessary. The following two commands provide methods for displaying speed and duplex information for switch ports. For information on displaying the currently configured port speed and duplex on

an LLDP-MED endpoint, refer to "Displaying the Current Port Speed and Duplex Configuration on a Switch Port" on page 5-64.

***Syntax:*** show interfaces brief < *port-list* >

*Includes port speed and duplex configuration in the* **Mode** *column of the resulting display.*

**Displaying Advertisements Currently in the Neighbors MIB.** These commands display the content of the inbound LLDP advertisements received from other LLDP devices.

***Syntax*** show lldp info remote-device [ *port-list* ]

*Without the [ port-list ] option, this command provides a global list of the individual devices it has detected by reading LLDP advertisements. Discovered devices are listed by the inbound port on which they were discovered. Multiple devices listed for a single port indicates that such devices are connected to the switch through a hub.*

*Discovering the same device on multiple ports indicates that the remote device may be connected to the switch in one of the following ways:*

- *Through different VLANS using separate links. (This applies to switches that use the same MAC address for all configured VLANs.)*
- *Through different links in the same trunk.*
- *Through different links using the same VLAN. (In this case, spanning-tree should be invoked to prevent a network topology loop. Note that LLDP packets travel on links that spanning-tree blocks for other traffic types.)*

*With the* [*port-list*] *option, this command provides a listing of the LLDP data that the switch has detected in advertisements received on the specified ports.*
*For descriptions of the various types of information displayed by these commands, refer to Table 5-3 on page 5-37.*

```
HP Switch(config)# show lldp info remote

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- ------------
  1         | 00 11 85 35 3b 80         6      6         Switch 2650
```

**Figure 5-24. Example of a Global Listing of Discovered Devices**

```
HP Switch(config)# show lldp info remote-device 1

 LLDP Remote Device Information Detail

  Local Port   : 1
  ChassisType  : network-address
  ChassisId    : 00 11 85 35 3b 80
  PortType     : mac-address
  PortId       : 08 00 0f 14 de f2
  SysName      : regDN 3004,<IP-Phone-Data>
  System Descr : regDN 3004,<IP-Phone-Data>,h/w rev 0,ASIC rev 0,f/w Boot FW...
  PortDescr    : LAN port

  System Capabilities Supported  : bridge, telephone
  System Capabilities Enabled    : bridge, telephone

  Remote Management Address
     Type    : ipv4
     Address : 192.192.1.2

  MED Information Detail
    EndpointClass           :Class3
    Media Policy Vlan id    :10
    Media Policy Priority   :7
    Media Policy Dscp       :44
    Media Policy Tagged     :False
    PoE Device Type         :PD
    Power Requested         :47
    Power Source            :Unknown
    Power Priority          :High
```

Indicates the policy configured on the telephone. A configuration mismatch occurs if the supporting port is configured differently.

**Figure 5-25. Example of an LLLDP-MED Listing of an Advertisement Received From an LLDP-MED (VoIP Telephone) Source**

## Displaying LLDP Statistics

LLDP statistics are available on both a global and a per-port levels. Rebooting the switch resets the LLDP statistics counters to zero. Disabling the transmit and/or receive capability on a port "freezes" the related port counters at their current values.

***Syntax*** show lldp stats [ *port-list* ]

*The global LLDP statistics command displays an overview of neighbor detection activity on the switch, plus data on the number of frames sent, received, and discarded per-port. The per-port LLDP statistics command enhances the list of per-port statistics provided by the global statistics command with some additional per-port LLDP statistics.*

Global LLDP Counters:

**Neighbor Entries List Last Updated:** *Shows the elapsed time since a neighbor was last added or deleted.*

**New Neighbor Entries Count:** *Shows the total of new LLDP neighbors detected since the last switch reboot. Disconnecting, then reconnecting a neighbor increments this counter.*

**Neighbor Entries Deleted Count:** *Shows the number of neighbor deletions from the MIB for AgeOut Count and forced drops for all ports. For example, if the admin status for port on a neighbor device changes from* **tx_rx** *or* **txonly** *to* **disabled** *or* **rxonly**, *then the neighbor device sends a "shutdown" packet out the port and ceases transmitting LLDP frames out that port. The device receiving the shutdown packet deletes all information about the neighbor received on the applicable inbound port and increments the counter.*

**Neighbor Entries Dropped Count:** *Shows the number of valid LLDP neighbors the switch detected, but could not add. This can occur, for example, when a new neighbor is detected when the switch is already supporting the maximum number of neighbors. Refer to "Neighbor Maximum" on page 5-69.*

**Neighbor Entries AgeOut Count:** *Shows the number of LLDP neighbors dropped on all ports due to Time-to-Live expiring.*

*— Continued —*

*— Continued —*

*Per-Port LLDP Counters:*

**NumFramesRecvd:** *Shows the total number of valid, inbound LLDP advertisements received from any neighbor(s) on <* port-list *>. Where multiple neighbors are connected to a port through a hub, this value is the total number of LLDP advertisements received from all sources.*

**NumFramesSent:** *Shows the total number of LLDP advertisements sent from <* port-list *>.*

**NumFramesDiscarded:** *Shows the total number of inbound LLDP advertisements discarded by <* port-list *>. This can occur, for example, when a new neighbor is detected on the port, but the switch is already supporting the maximum number of neighbors. Refer to "Neighbor Maximum" on page 5-69. This can also be an indication of advertisement formatting problems in the neighbor device.*

**Frames Invalid:** *Shows the total number of invalid LLDP advertisements received on the port. An invalid advertisement can be caused by header formatting problems in the neighbor device.*

**TLVs Unrecognized:** *Shows the total number of LLDP TLVs received on a port with a type value in the reserved range. This could be caused by a basic management TLV from a later LLDP version than the one currently running on the switch.*

**TLVs Discarded:** *Shows the total number of LLDP TLVs discarded for any reason. In this case, the advertisement carrying the TLV may be accepted, but the individual TLV was not usable.*

**Neighbor Ageouts:** *Shows the number of LLDP neighbors dropped on the port due to Time-to-Live expiring.*

```
HP Switch(config)# show lldp stats

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2 hours
  New Neighbor Entries Count : 20
  Neighbor Entries Deleted Count : 20
  Neighbor Entries Dropped Count : 0
  Neighbor Entries AgeOut Count : 20

 LLDP Port Statistics

  Port | NumFramesRecvd NumFramesSent NumFramesDiscarded
  ---- + -------------- ------------- -----------------
  1    | 628            316           0
  2    | 21             12            0
  3    | 0              252           0
  4    | 446            226           0
  5    | 0              0             0
  .    | .              .             .
  .    | .              .             .
  .    | .              .             .
```

Counters showing frames sent on a port but no frames received on that port indicates an active link with a device that either has LLDP disabled on the link or is not LLDP-aware.

**Figure 5-26. Example of a Global LLDP Statistics Display**

```
HP Switch(config)# show lldp stats
1

 LLDP Port Statistics Detail

  PortName : 1
  Frames Discarded  : 0
  Frames Invalid    : 0
  Frames Received   : 658
  Frames Sent       : 331
  TLVs Unrecognized : 0
  TLVs Discarded    : 0
  Neighbor Ageouts  : 0
```

**Figure 5-27. Example of a Per-Port LLDP Statistics Display**

## LLDP Operating Notes

**Neighbor Maximum.** The neighbors table in the switch supports as many neighbors as there are ports on the switch. The switch can support multiple neighbors connected through a hub on a given port, but if the switch neighbor maximum is reached, advertisements from additional neighbors on the same or other ports will not be stored in the neighbors table unless some existing neighbors time-out or are removed.

**LLDP Packet Forwarding:** An 802.1D-compliant switch does not forward LLDP packets, regardless of whether LLDP is globally enabled or disabled on the switch.

**One IP Address Advertisement Per-Port:** LLDP advertises only one IP address per-port, even if multiple IP addresses are configured by **lldp config < *port-list* > ipAddrEnable** on a given port.

**802.1Q VLAN Information.** LLDP packets do not include 802.1Q header information, and are always handled as untagged packets.

**Effect of 802.1X Operation.** If 802.1X port security is enabled on a port and a connected device is not authorized, LLDP packets are not transmitted or received on that port. Any neighbor data stored in the neighbor MIB for that port prior to the unauthorized device connection remains in the MIB until it ages out. If an unauthorized device later becomes authorized, LLDP transmit and receive operation resumes.

**Neighbor Data Can Remain in the Neighbor Database After the Neighbor Is Disconnected.** After disconnecting a neighbor LLDP device from the switch, the neighbor can continue to appear in the switch's neighbor database for an extended period if the neighbor's **holdtime-multiplier** is high; especially if the **refresh-interval** is large. Refer to "Changing the Time-to-Live for Transmitted Advertisements" on page 5-43.

**Mandatory TLVs.** All mandatory TLVs required for LLDP operation are also mandatory for LLDP-MED operation.

**Determining the Switch Port Number Included in Topology Change Notification Traps.** Enabling topology change notification on a switch port and then connecting or disconnecting an LLDP-MED endpoint on that port causes the switch to send an SNMP trap to notify the designated management station(s). The port number included in the trap corresponds to the internal number the switch maintains for the designated port, and not the port's external identity. To match the port's external number to the internal port number appearing in an SNMP trap, use the **walkmib ifDescr** command, as shown in the following figure:

```
 HP Switch# walkmib ifDescr
ifDescr.1 = 1
ifDescr.2 = 2
ifDescr.3 = 3
.
.
.
ifDescr.23 = 23
ifDescr.24 = 24
```

**Figure 5-28. Matching Internal Port Numbers to External Port Numbers for Modular Switches**

# LLDP and CDP Data Management

This section describes points to note regarding LLDP (Link-Layer Discovery Protocol) and CDP (Cisco Discovery Protocol) data received by the switch from other devices. LLDP operation includes both transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices. CDP operation is limited to reading incoming CDP packets from neighbor devices. (HP switches do not generate CDP packets.)

## LLDP and CDP Neighbor Data

With both LLDP and (read-only) CDP enabled on a switch port, the port can read both LLDP and CDP advertisements, and stores the data from both types of advertisements in its neighbor database. (The switch only *stores* CDP data that has a corresponding field in the LLDP neighbor database.) The neighbor database itself can be read by either LLDP or CDP methods or by using the **show lldp** commands. Take note of the following rules and conditions:

- If the switch receives both LLDP and CDP advertisements on the same port from the same neighbor the switch stores this information as two separate entries if the advertisements have differences chassis ID and port ID information.
- If the chassis and port ID information are the same, the switch stores this information as a single entry. That is, LLDP data overwrites the corresponding CDP data in the neighbor database if the chassis and port ID information in the LLDP and CDP advertisements received from the same device is the same.
- Data read from a CDP packet does not support some LLDP fields, such as “System Descr”, “SystemCapSupported”, and “ChassisType”. For such fields, LLDP assigns relevant default values. Also:
  - The LLDP “System Descr” field maps to CDP’s “Version” and “Platform” fields.
  - The switch assigns “ChassisType” and “PortType” fields as “local” for both the LLDP and the CDP advertisements it receives.
  - Both LLDP and CDP support the “System Capability” TLV. However, LLDP differentiates between what a device is capable of supporting and what it is actually supporting, and separates the two types of information into subelements of the System Capability TLV. CDP has only a single field for this data. Thus, when CDP System Capability data is mapped to LLDP, the same value appears in both LLDP System Capability fields.
  - System Name and Port Descr are not communicated by CDP, and thus are not included in the switch’s Neighbors database.

**Note**

Because HP switches do not generate CDP packets, they are not represented in the CDP data collected by any neighbor devices running CDP.

A switch with CDP disabled forwards the CDP packets it receives from other devices, but does not store the CDP information from these packets in its own MIB.

LLDP data transmission/collection and CDP data collection are both enabled in the switch's default configuration. In this state, an SNMP network management application designed to discover devices running either CDP or LLDP can retrieve neighbor information from the switch regardless of whether LLDP or CDP is used to collect the device-specific information.

| Protocol State | Packet Generation | Inbound Data Management | Inbound Packet Forwarding |
|---|---|---|---|
| CDP Enabled[1] | n/a | Store inbound CDP data. | No forwarding of inbound CDP packets. |
| CDP Disabled | n/a | No storage of CDP data from neighbor devices. | Floods inbound CDP packets from connected devices to outbound ports. |
| LLDP Enabled[1] | Generates and transmits LLDP packets out all ports on the switch. | Store inbound LLDP data. | No forwarding of inbound LLDP packets. |
| LLDP Disabled | No packet generation. | No storage of LLDP data from neighbor devices. | No forwarding of inbound LLDP packets. |

[1] Both CDP data collection and LLDP transmit/receive are enabled in the default configuration. If a switch receives CDP packets and LLDP packets from the same neighbor device on the same port, it stores and displays the two types of information separately if the chassis and port ID information in the two types of advertisements is different. In this case, if you want to use only one type of data from a neighbor sending both types, disable the unwanted protocol on either the neighbor device or on the switch. However, if the chassis and port ID information in the two types of advertisements is the same, the LLDP information overwrites the CDP data for the same neighbor device on the same port.

## CDP Operation and Commands

By default the switches covered in this guide have CDP enabled on each port. This is a read-only capability, meaning that the switch can receive and store information about adjacent CDP devices but does not generate CDP packets.

When a CDP-enabled switch receives a CDP packet from another CDP device, it enters that device's data in the CDP Neighbors table, along with the port number where the data was received (and does not forward the packet). The switch also periodically purges the table of any entries that have expired. (The hold time for any data entry in the switch's CDP Neighbors table is configured in the device transmitting the CDP packet, and cannot be controlled in the switch receiving the packet.) A switch reviews the list of CDP neighbor entries every three seconds, and purges any expired entries.

| Command | Page |
|---|---|
| show cdp | 5-73 |
| show cdp neighbors [< *port-list* > detail] [detail < *port-list* >] | 5-74 |
| [no] cdp run | 5-74 |
| [no] cdp enable < *port-list* > | 5-75 |

**Note**

For details on how to use an SNMP utility to retrieve information from the switch's CDP Neighbors table maintained in the switch's MIB (Management Information Base), refer to the documentation provided with the particular SNMP utility.

**Viewing the Switch's Current CDP Configuration.** CDP is shown as enabled/disabled both globally on the switch and on a per-port basis.

***Syntax:*** show cdp

*Lists the switch's global and per-port CDP configuration.*

The following example shows the default CDP configuration.

```
HP Switch(config)# show cdp

 Global CDP information

  Enable CDP [Yes] : Yes (Receive Only)


  Port CDP
  ---- --------
  1    enabled
  2    enabled
  3    enabled
  .       .
  .       .
  .       .
```

**Figure 5-29. Example of Show CDP with the Default CDP Configuration**

**Viewing the Switch's Current CDP Neighbors Table.** Devices are listed by the port on which they were detected.

***Syntax:*** show cdp neighbors

*Lists the neighboring CDP devices the switch detects, with a subset of the information collected from the device's CDP packet.*

[ [e] port-num [detail] ]

*Lists the CDP device connected to the specified port. (Allows only one port at a time.) Using* **detail** *provides a longer list of details on the CDP device the switch detects on the specified port.*

[detail [ [e] port-num ] ]

*Provides a list of the details for all of the CDP devices the switch detects. Using port-num produces a list of details for the selected port.*

Figure 5-30 lists CDP devices that the switch has detected by receiving their CDP packets.

```
HP Switch> show cdp neighbors

 CDP neighbors information

  Port Device ID                    | Platform                    Capability
  ---- ---------------------------- + --------------------------- ----------
  1    Accounting(0030c1—7fcc40)    | J4812A HP Switch...         S
  2    Research(0060b0—889e43)      | J4121A HP Switch...         S
  4    Support(0060b0—761a45)       | J4121A HP Switch...         S
  7    Marketing(0030c5—38dc59)     | J4813A HP Switch...         S
  12   Mgmt NIC(099a05—09df9b       | NIC Model X666              M
  12   Mgmt NIC(099a05—09df11       | NIC Model X666              M
```

**Figure 5-30. Example of CDP Neighbors Table Listing**

**Enabling CDP Operation.** Enabling CDP operation (the default) on the switch causes the switch to add entries to its CDP Neighbors table for any CDP packets it receives from other neighboring CDP devices.

**Disabling CDP Operation.** Disabling CDP operation clears the switch's CDP Neighbors table and causes the switch to drop inbound CDP packets from other devices without entering the data in the CDP Neighbors table.

***Syntax:*** [no] cdp run

*Enables or disables CDP read-only operation on the switch. (Default: Enabled)*

For example, to disable CDP read-only on the switch:

```
HP Switch(config)# no cdp run
```

When CDP is disabled:

- **show cdp neighbors** displays an empty CDP Neighbors table
- **show cdp** displays

```
Global CDP information
 Enable CDP [Yes]: No
```

**Enabling or Disabling CDP Operation on Individual Ports.** In the factory-default configuration, the switch has all ports enabled to receive CDP packets. Disabling CDP on a port causes it to drop inbound CDP packets without recording their data in the CDP Neighbors table.

***Syntax:*** [no] cdp enable < [e] port-list >

For example, to disable CDP on port 1:

```
HP Switch(config)# no cdp enable 1
```

# File Transfers

The switches covered in this guide support several methods for transferring files to and from a physically connected device, or via the network, including TFTP and Xmodem. This appendix explains how to download new switch software, upload or download switch configuration files and software images. It contains the following information:

- Downloading switch software (begins on this page)
- Copying software images (page A-19)
- Transferring switch configurations (begins on page A-20)
- Copying diagnostic data (begins on page A-24)

## Downloading Switch Software

HP periodically provides switch software updates through the HP web site. For more information, refer to the support and warranty booklet shipped with the switch, or visit **www.hp.com/Networking/support** and click on **software updates**. After you acquire a new software version, you can use one of the following methods for downloading software to the switch:

| Software Download Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| TFTP | n/a | page A-2 | page A-5 | — |
| Xmodem | n/a | page A-15 | page A-16 | — |
| Switch-to-Switch | n/a | page A-17 | page A-18 | — |
| Software Update Manager in IMC | Refer to the documentation provided with IMC. | | | |

**Note**

This manual uses the terms *switch software* and *software image* to refer to the downloadable software files the switch uses to operate its networking features. Other terms sometimes include *Operating System*, or *OS*.

### General Software Download Rules

- Switch software that you download via the menu interface always goes to primary flash.
- After a software download, you must reboot the switch to implement the new software. Until a reboot occurs, the switch continues to run on the software it was using before the download commenced.

**Note**

Downloading new switch software does not change the current switch configuration. The switch configuration is contained in separate files that can also be transferred. Refer to "Transferring Switch Configurations" on page A-19.

In most cases, if a power failure or other cause interrupts a flash image download, the switch reboots with the image previously stored in primary flash. In the unlikely event that the primary image is corrupted (which may occur if a download is interrupted by a power failure), the switch goes into boot ROM mode. In this case, use the boot ROM console to download a new image to primary flash. Refer to "Restoring a Flash Image" on page C-61.

## Using TFTP To Download Switch Software from a Server

This procedure assumes that:

- A software version for the switch has been stored on a TFTP server accessible to the switch. (The software file is typically available from the HP web site at **www.hp.com/Networking/support**.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the software file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the software file stored in the TFTP server for the switch (for example, E0820.swi).

**Note**

If your TFTP server is a UNIX workstation, *ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the software filenames on the server.*

### Menu: TFTP Download from a Server to Primary Flash

Note that the menu interface accesses only the primary flash.

1. In the console Main Menu, select **Download OS** to display the screen in figure A-1. (The term "OS", or "operating system" refers to the switch software):

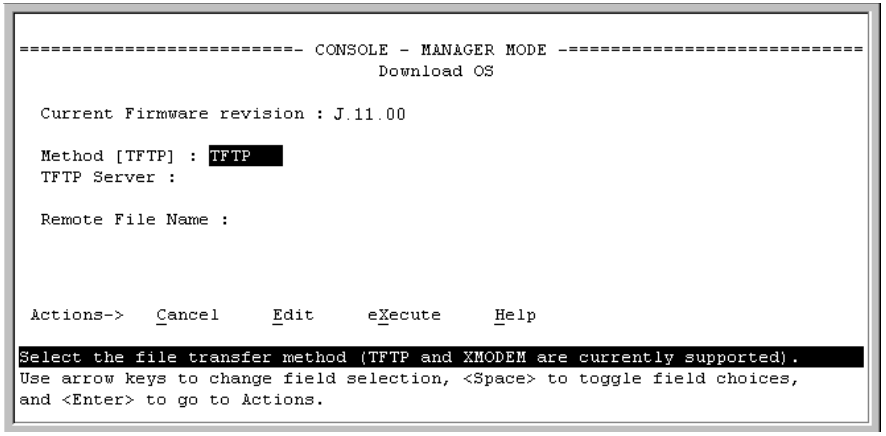



**Figure A-1. Example of a Download OS (Software) Screen (Default Values)**

2. Press **[E]** (for **Edit**).
3. Ensure that the **Method** field is set to **TFTP** (the default).
4. In the **TFTP Server** field, type in the IP address of the TFTP server in which the software file has been stored.
5. In the **Remote File Name** field, type the name of the software file. If you are using a UNIX system, remember that the filename is case-sensitive.
6. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download. The followingscreenthenappears:

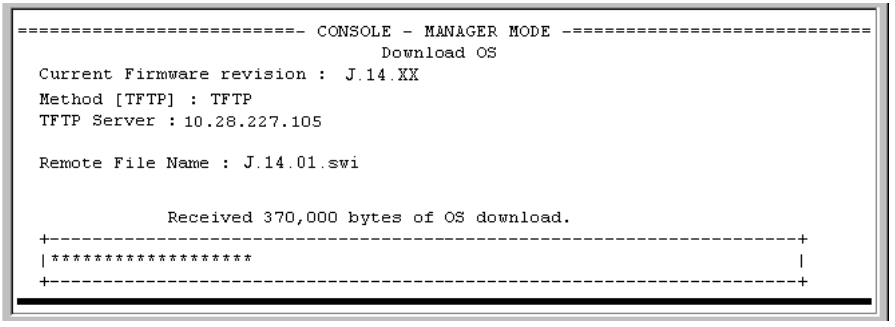



**Figure A-2. Example of the Download OS (Software) Screen During a Download**

A "progress" bar indicates the progress of the download. When the entire software file has been received, all activity on the switch halts and you will see **Validating and writing system software to FLASH...**

7. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see this prompt:

   ```
   Continue reboot of system?  :  No
   ```

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

**Note**

When you use the menu interface to download a switch software, the new image is always stored in primary flash. Also, using the Reboot Switch command in the Main Menu always reboots the switch from primary flash. Rebooting the switch from the CLI gives you more options. Refer to *Basic Operation Guide*.

8. After you reboot the switch, confirm that the software downloaded correctly:
   a. From the Main Menu, select **1. Status and Counters**, and from the Status and Counters menu, select **1. General System Information**
   b. Check the **Firmware revision** line.

**Troubleshooting TFTP Download Failures.** When using the menu interface, if a TFTP download fails, the Download OS (Operating System, or software) screen indicates the failure.

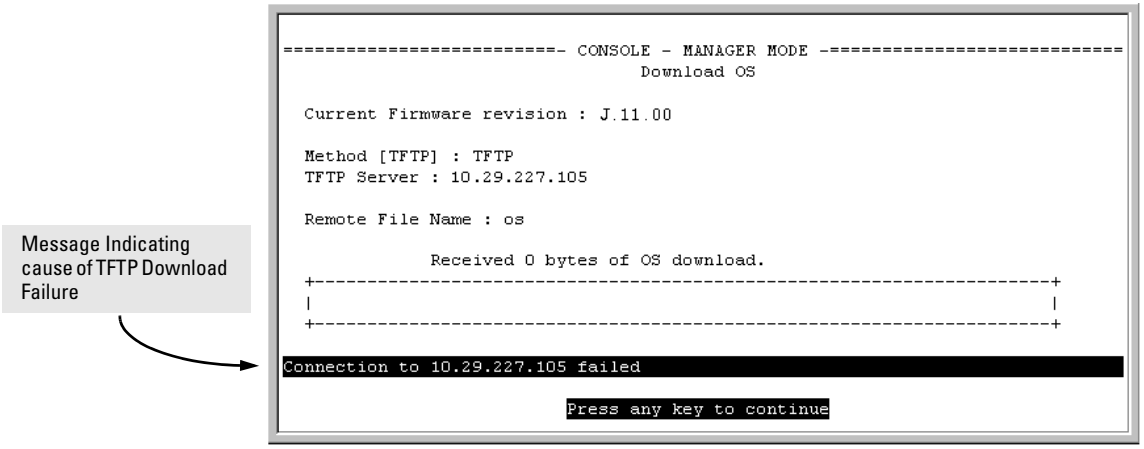



**Figure A-3. Example of Message for Download Failure**

To find more information on the cause of a download failure, examine the messages in the switch's Event Log by executing the **show log tftp** command from the CLI. Also:

- For more on the Event Log, see "Using the Event Log for Troubleshooting Switch Problems" on page C-17.
- For descriptions of individual Event Log messages, refer to the latest version of the *Event Log Message Reference Guide* for your switch, available on the HPNetworking website. (See also *Basic Operation Guide*.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a UNIX machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the **Download OS** (Operating System, or software) screen.
- One or more of the switch's IP configuration parameters are incorrect.
- For a UNIX TFTP server, the file permissions for the software file do not allow the file to be copied.
- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

**Note**

If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself. In this case, an appropriate message is displayed after the switch reboots.

## CLI: TFTP Download from a Server to Flash

***Syntax:*** copy tftp flash <*ip-address*> <*remote-file*> [< primary | secondary >]

*This command automatically downloads a switch software file to primary or secondary flash. Note that if you do not specify the flash destination, the TFTP download defaults to primary flash.*

For example, to download a switch software file named k0800.swi from a TFTP server with the IP address of 10.28.227.103 to primary flash:

1. Execute **copy** as shown below:

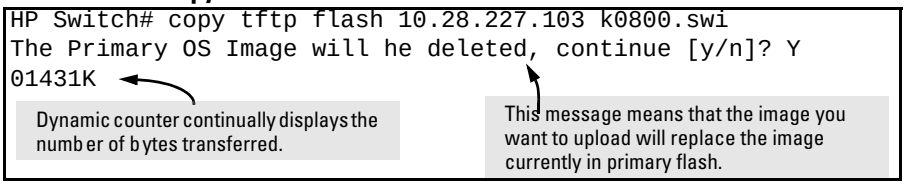



**Figure A-4. Example of the Command to Download an OS (Switch Software)**

2. When the switch finishes downloading the software file from the server, it displays this progress message:

   **Validating and Writing System Software to FLASH ...**

3. When the download finishes, you must reboot the switch to implement the newly downloaded software image. To do so, use one of the following commands:

   ***Syntax:*** boot system flash < primary | secondary >

   *Boots from the selected flash.*

   ***Syntax:*** reload

   *Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.*

   (For more on these commands, refer to *Basic Operation Guide*.)

4. To confirm that the software downloaded correctly, execute **show system** and check the Firmware revision line.

For information on primary/secondary flash memory and the boot commands, refer to *Basic Operation Guide*.

## Using Secure Copy and SFTP

For some situations you may want to use a secure method to issue commands or copy files to the switch. By opening a secure, encrypted SSH session you can then use a third-party software application to take advantage of Secure Copy (SCP) and Secure ftp (SFTP). SCP and SFTP provide a secure alternative to TFTP for transferring information that may be sensitive (like switch configuration files) to and from the switch. Essentially you are creating a secure SSH tunnel as a way to transfer files with SFTP and SCP channels.

To use these commands you must install on the administrator workstation a third-party application software client that supports the SFTP and/or SCP functions. Some examples of software that supports SFTP and SCP are PuTTY, Open SSH, WinSCP, and SSH Secure Shell. Most of these are freeware and may be downloaded without cost or licensing from the internet. There are differences in the way these clients work, so be sure you also download the documentation.

As described earlier in this chapter you can use a TFTP client on the administrator workstation to update software images. This is a plain text mechanism and it connects to a standalone TFTP server or another HP switch acting as a TFTP server to obtain the software image file(s). Using SCP and SFTP allows you to maintain your switches with greater security. You can also roll out new software images with automated scripts that make it easier to upgrade multiple switches simultaneously and securely.

SFTP (secure file transfer protocol) is unrelated to FTP, although there are some functional similarities. Once you set up an SFTP session through an SSH tunnel, some of the commands are the same as FTP commands. Certain commands are not allowed by the SFTP server on the switch, such as those that create files or folders. If you try to issue commands such as **create** or **remove** using SFTP the switch server returns an error message.

You can use SFTP just as you would TFTP to transfer files to and from the switch, but with SFTP your file transfers are encrypted and require authentication, so they are more secure than they would be using TFTP. SFTP works only with SSH version 2 (SSH v2).

**Note**

SFTP over SSH version 1 (SSH v1) is not supported. A request from either the client or the switch (or both) using SSH v1 generates an error message. The actual text of the error message differs, depending on the client software in use. Some examples are:

```
Protocol major versions differ: 2 vs. 1
Connection closed
```

```
Protocol major versions differ: 1 vs. 2
Connection closed
```

```
Received disconnect from <ip-addr>: /usr/local/
libexec/sftp-server: command not supported
Connection closed
```

SCP (secure copy) is an implementation of the BSD **rcp** (Berkeley UNIX remote copy) command tunneled through an SSH connection.

SCP is used to copy files to and from the switch when security is required. SCP works with both SSH v1 and SSH v2. Be aware that the most third-party software application clients that support SCP use SSHv1.

### How It Works

The general process for using SCP and SFTP involves three steps:

1. Open an SSH tunnel between your computer and the switch if you haven't already done so. (This step assumes that you have already set up SSH on the switch.)
2. Execute **ip ssh filetransfer** to tell the switch that you want to enable secure file transfer.
3. Use a third-party client application for SCP and SFTP commands.

## The SCP/SFTP Process

To use SCP and SFTP:

1. Open an SSH session as you normally would to establish a secure encrypted tunnel between your computer and the switch. For more detailed directions on how to open an SSH session refer to the chapter titled *"Configuring Secure Shell (SSH)"* in the *Access Security Guide* for your switch. Please note that this is a one-time procedure for new switches or connections. If you have already done it once you should not need to do it a second time.
2. To enable secure file transfer on the switch (once you have an SSH session established between the switch and your computer), open a terminal window and type in the following command:

   ```
   HP Switch(config)# ip ssh filetransfer
   ```

### Disable TFTP and Auto-TFTP for Enhanced Security

Using the **ip ssh filetransfer** command to enable Secure FTP (SFTP) automatically disables TFTP and auto-TFTP (if either or both are enabled).

```
HP Switch(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled.
HP Switch(config)# sho run

Running configuration:

; J9229A Configuration Editor; Created on release #YA.15.XX

hostname "Switch"
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address 10.28.234.176 255.255.240.0
   exit
ip ssh filetransfer
no tftp-enable
password manager
password operator
```

Enabling SFTP automatically disables TFTP and auto-tftp and displays this message.

Viewing the configuration shows that SFTP is enabled and TFTP is disabled.

**Figure A-5. Example of Switch Configuration with SFTP Enabled**

If you enable SFTP, then later disable it, TFTP and auto-TFTP remain disabled unless they are explicitly re-enabled.

Operating rules are:

- The TFTP feature is enabled by default, and can be enabled or disabled through the CLI, the Menu interface, or an SNMP application. Auto-TFTP is disabled by default and must be configured through the CLI.

```
============================= CONSOLE - MANAGER MODE ==============================
                  Switch Configuration - System Information

  System Name : Switch
  System Contact :
  System Location :

  Inactivity Timeout (min) [0] : 0       MAC Age Time (sec) [300] : 300
  Inbound Telnet Enabled [Yes] : Yes     Web Agent Enabled [Yes] : Yes
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled
  Tftp-enable [Yes] : Yes

  Time Zone [0] : 0
  Daylight Time Rule [None] : None


 Actions->   Cancel     Edit      Save      Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Enables/Disables TFTP.

**Note:** If SFTP is enabled, this field will be set to **No**. You cannot use this field to enable TFTP if SFTP is enabled. Attempting to do so produces an **Inconsistent value** message in the banner below the **Actions** line.

**Figure A-6. Using the Menu Interface To Disable TFTP**

- While SFTP is enabled, TFTP and auto-TFTP cannot be enabled from the CLI. Attempting to enable either non-secure TFTP option while SFTP is enabled produces one of the following messages in the CLI:

```
SFTP must be disabled before enabling tftp.

SFTP must be disabled before enabling auto-tftp.
```

  Similarly, while SFTP is enabled, TFTP cannot be enabled using an SNMP management application. Attempting to do so generates an "inconsistent value" message. (An SNMP management application cannot be used to enable or disable auto-TFTP.)

- To enable SFTP by using an SNMP management application, you must first disable TFTP and, if configured, auto-TFTP on the switch. You can use either an SNMP application or the CLI to disable TFTP, but must use the CLI to disable auto-TFTP. The following two CLI commands disable TFTP and auto-TFTP on the switch.

***Syntax:*** no tftp-enable

*This command disables all TFTP operation on the switch except for the auto-TFTP feature. To re-enable TFTP operation, use the* **tftp-enable** *command. When TFTP is disabled, the instances of* **tftp** *in the CLI copy command and the Menu interface "Download OS" screen become unavailable.*

***Note:*** *This command does* ***not*** *disable auto-TFTP operation. To disable an auto-TFTP command configured on the switch, use the* **no auto-tftp** *command described below to remove the command entry from the switch's configuration.*

***Syntax:*** no auto-tftp

*If auto-TFTP is configured on the switch, this command deletes the* **auto-tftp** *entry from the switch configuration, thus preventing auto-tftp operation if the switch reboots.*

***Note:*** *This command does not affect the current TFTP-enable configuration on the switch.*

## Command Options

If you need to enable SSH v2 (which is required for SFTP) enter this command:

```
HP Switch(config)# ip ssh version 2
```

**Note**

As a matter of policy, administrators should *not* enable the SSHv1-only or the SSHv1-or-v2 advertisement modes. SSHv1 is supported on only some legacy switches (such as the HP Series 2500 switches).

To confirm that SSH is enabled type in the command

```
HP Switch(config)# show ip ssh
```

Once you have confirmed that you have enabled an SSH session (with the **show ip ssh** command) you can then open your third-party software client application to begin using the SCP or SFTP commands to safely transfer files or issue commands to the switch.

If you need to disable secure file transfer:

```
HP Switch(config)# no ip ssh filetransfer
```

## Authentication

Switch memory allows up to ten public keys. This means the authentication and encryption keys you use for your third-party client SCP/SFTP software can differ from the keys you use for the SSH session, even though both SCP and SFTP use a secure SSH tunnel.

**Note** SSH authentication is mutually exclusive with RADIUS servers.

Some clients such as PSCP (PuTTY SCP) automatically compare switch host keys for you. Other clients require you to manually copy and paste keys to the **$HOME/.ssh/known_hosts** file. Whatever SCP/SFTP software tool you use, after installing the client software you must verify that the switch host keys are available to the client.

Because the third-party software utilities you may use for SCP/SFTP vary, you should refer to the documentation provided with the utility you select before performing this process.

## SCP/SFTP Operating Notes

- Any attempts to use SCP or SFTP without using **ip ssh filetransfer** will cause the SCP or SFTP session to fail. Depending on the client software in use, you will receive an error message on the originating console, for example:

  ```
  IP file transfer not enabled on the switch
  ```

- There is a delay when SFTP is copying an image onto the switch, and although the command prompt returns in a couple of seconds, the switch may take approximately a minute and half writing the image to flash. You can keep entering the **show flash** command to see when the copy is complete and the flash is updated. You can also check the log for an entry similar to the following:

```
I 01/09/09 16:17:07 00150 update: Primary Image
updated.

I 01/09/09 16:13:22 00636 ssh: sftp session from
12.22.22.03
```

- When an SFTP client connects, the switch provides a file system displaying all of its available files and folders. No file or directory creation is permitted by the user. Files may only be uploaded or downloaded, according to the permissions mask. All of the necessary files the switch will need are already in place on the switch. You do not need to (nor can you create) new files.
- The switch supports one SFTP session or one SCP session at a time.
- All files have read-write permission. Several SFTP commands, such as `create` or `remove`, are not allowed and return an error message. The switch displays the following files:

```
/
+---cfg
|   running-config
|   startup-config
+---log
|   crash-data
|   crash-data-a
|   crash-data-b
|   crash-data-c
|   crash-data-e          “             “
|   crash-data-f          “             “
|   crash-data-h          “         “
|   crash-data-I          “         “
|   crash-data-J          “         “
|   crash-data-K          “         “
|   crash-data-L          “         “
|   crash-log
|   crash-log-a
|   crash-log-b
|   crash-log-c
|   crash-log-e          “             “
|   crash-log-f          “             “
|   crash-log-h          “        “
|   crash-log-I          “        “
|   crash-log-J          “        “
|   crash-log-K          “        “
|   crash-log-L          “        “
|   event log
+---os
|   primary
|   secondary
```

```
\---ssh
    +---mgr_keys
    |   authorized_keys
    \---oper_keys
        authorized_keys
```

Once you have configured your switch for secure file transfers with SCP and SFTP, files can be copied to or from the switch in a secure (encrypted) environment and TFTP is no longer necessary.

## Troubleshooting SSH, SFTP, and SCP Operations

You can verify secure file transfer operations by checking the switch's event log, or by viewing the error messages sent by the switch that most SCP and SFTP clients will print out on their console.

**Note** Messages that are sent by the switch to the client depend on the client software in use to display them on the user console.

**Broken SSH Connection.** If an ssh connection is broken at the wrong moment (for instance, the link goes away or spanning tree brings down the link), a fatal exception would occur on the switch. If this happens, the switch will gracefully exit the session and produce an event log message indicating the cause of failure. The following three examples show the error messages that may appear in the log depending on the type of session that is running (SSH, SCP, or SFTP).

```
ssh: read error Bad file number, session aborted I 01/
01/90 00:06:11 00636 ssh: sftp session from
::ffff:10.0.12.35 W 01/01/90 00:06:26 00641 ssh:
```

```
sftp read error Bad file number, session aborted I 01/
01/90 00:09:54 00637 ssh: scp session from
::ffff:10.0.12.35 W 01/01/90
```

```
ssh: scp read error Bad file number, session aborted
```

**Note** The `Bad file number` is from the system error value and may differ depending on the cause of the failure. In the third example, the device file to read was closed as the device read was about to occur.

**Attempt to Start a Session During a Flash Write.** If you attempt to start an SCP (or SFTP) session while a flash write is in progress, the switch will not allow the SCP or SFTP session to start. Depending on the client software in use, the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Flash access
in progress

lost connection
```

**Failure to Exit from a Previous Session.** This next example shows the error message that may appear on the client console if a new SCP (or SFTP) session is started from a client before the previous client session has been closed (the switch requires approximately ten seconds to timeout the previous session):

```
Received disconnect from 10.0.12.31: 2: Wait for
previous session to complete

lost connection
```

**Attempt to Start a Second Session.** The switch supports only one SFTP session or one SCP session at a time. If a second session is initiated (for example, an SFTP session is running and then an SCP session is attempted), then the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Other SCP/SFTP
session running

lost connection
```

## Using Xmodem to Download Switch Software From a PC or UNIX Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the *Installation and Getting Started Guide* you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the **Send File** option in the **Transfer** dropdown menu.)

## Menu: Xmodem Download to Primary Flash

Note that the menu interface accesses only the primary flash.

1. From the console Main Menu, select

   **7. Download OS**

2. Press **[E]** (for **Edit**).

3. Use the Space bar to select **XMODEM** in the **Method** field.

4. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download. The following message then appears:

   **Press enter and then initiate Xmodem transfer**
   **from the attached computer.....**

5. Press **[Enter]** and then execute the terminal emulator command(s) to begin Xmodem binary transfer. For example, using HyperTerminal:

   a. Click on **Transfer**, then **Send File**.

   b. Type the file path and name in the Filename field.

   c. In the Protocol field, select **Xmodem**.

   d. Click on the **[Send]** button.

   The download will then commence. It can take several minutes, depending on the baud rate set in the switch and in your terminal emulator.

6. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see the following prompt:

   **Continue reboot of system? : No**

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

7. To confirm that the software downloaded correctly:

   a. From the Main Menu, select

      **1. Status and Counters**

         **1. General System Information**

   b. Check the **Firmware revision** line.

## CLI: Xmodem Download from a PC or UNIX Workstation to Primary or Secondary Flash

Using Xmodem and a terminal emulator, you can download a software file to either primary or secondary flash.

***Syntax:*** copy xmodem flash [< primary | secondary >]

*Downloads a software file to primary or secondary flash. If you do not specify the flash destination, the Xmodem download defaults to primary flash.*

For example, to download a switch software file named E0822.swi from a PC (running a terminal emulator program such as HyperTerminal) to primary flash:

1. Execute the following command in the CLI:

```
HP Switch# copy xmodem flash
The Primary OS Image will be deleted, continue [y/n]? Y
Press 'Enter' and start XMODEM on your host...
```

2. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
   a. Click on **Transfer**, then **Send File**.
   b. Type the file path and name in the Filename field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **[Send]** button.

   The download can take several minutes, depending on the baud rate used in the transfer.

3. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

   ***Syntax:*** boot system flash <primary | secondary>

   *Reboots from the selected flash.*

   ***Syntax:*** reload

   *Reboots from the flash image currently in use.*

   (For more on these commands, see *Basic Operation Guide*.)

# Switch-to-Switch Download

You can use TFTP to transfer a software image between two switches of the same series. The menu interface enables you to transfer primary-to-primary or secondary-to-primary. The CLI enables all combinations of flash location options.

## Menu: Switch-to-Switch Download to Primary Flash

Using the menu interface, you can download a switch software file from either the primary or secondary flash of one switch to the primary flash of another switch of the same series.

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS** screen.
2. Ensure that the **Method** parameter is set to **TFTP** (the default).
3. In the **TFTP Server** field, enter the IP address of the remote switch containing the software file you want to download.
4. For the **Remote File Name**, enter one of the following:
   - To download the software in the primary flash of the source switch, type "**flash**" in lowercase characters.
   - To download the software in the secondary flash of the source switch, type **/os/secondary**.
5. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download.
6. A "progress" bar indicates the progress of the download. When the entire switch software download has been received, all activity on the switch halts and the following messages appear:

   **Validating and writing system software to FLASH...**
7. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You will then see this prompt:

   **Continue reboot of system? : No**

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.
8. To confirm that the software downloaded correctly:
   a. From the Main Menu, select

**Status and Counters**

**General System Information**

b. Check the **Firmware revision** line.

## CLI: Switch-To-Switch Downloads

Where two switches in your network belong to the same series, you can download a software image between them by initiating a **copy tftp** command from the destination switch. The options for this CLI feature include:

- Copy from primary flash in the source to either primary or secondary in the destination.
- Copy from either primary or secondary flash in the source to either primary or secondary flash in the destination.

**Downloading from Primary Only.**

***Syntax:*** copy tftp flash < *ip-addr* > flash [ primary | secondary ]

*This command (executed in the destination switch) downloads the software flash in the source switch's primary flash to either the primary or secondary flash in the destination switch.*

If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

For example, to download a software file from primary flash in a switch with an IP address of 10.29.227.103 to the primary flash in the destination switch, you would execute the following command in the destination switch's CLI:

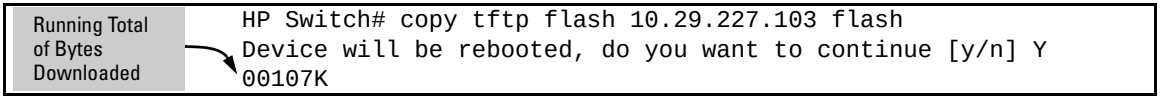



**Figure A-7. Switch-To-Switch, from Primary in Source to Either Flash in Destination**

**Downloading from Either Flash in the Source Switch to Either Flash in the Destination Switch.**

***Syntax:*** copy tftp flash < *ip-addr* > < /os/primary > | < /os/secondary > [ primary | secondary ]

*This command (executed in the destination switch) gives you the most options for downloading between switches. If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.*

For example, to download a software file from secondary flash in a switch with an IP address of 10.28.227.103 to the secondary flash in a destination switch, you would execute the following command in the destination switch's CLI:

```
HP Switch# copy tftp flash 10.29.227.103 /os/secondary second-
ary
Device will be rebooted, do you want to continue [y/n] Y
```

**Figure A-8. Switch-to-Switch, from Either Flash in Source to Either Flash in Destination**

## Using IMC to Update Switch Software

IMC includes a software update utility for updating on HP switch products. For further information, refer to the *Basic Operation Guide* and the *Administrator's Guide*, provided electronically with the application.

# Copying Software Images

Using the CLI commands described in this section, you can copy software images from the switch to another device using tftp or xmodem.

**Note**

For details on how switch memory operates, including primary and secondary flash, refer to *Basic Operation Guide*.

### TFTP: Copying a Software Image to a Remote Host

***Syntax:*** copy flash tftp < *ip-addr* > < *filename* >

*This command copies the primary flash image to a TFTP server.*

For example, to copy the primary flash to a TFTP server having an IP address of 10.28.227.105:

```
HP Switch# copy flash tftp 10.28.227.105 k0800.swi
```

where `k0800.swi` is the filename given to the flash image being copied.

### Xmodem: Copying a Software Image from the Switch to a Serially Connected PC or UNIX Workstation

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation.

***Syntax:*** copy flash xmodem < pc | unix >

*Uses Xmodem to copy a designated configuration file from the switch to a PC or Unix workstation.*

For example, to copy the primary flash image to a serially connected PC:

1. Execute the following command:

```
HP Switch# copy xmodem flash
Press 'Enter' and start XMODEM on your host...
```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.

## Transferring Switch Configurations

**Transfer Features**

| Feature | Page |
|---|---|
| Use TFTP to copy from a remote host to a config file. | A-21 |
| Use TFTP to copy a config file to a remote host. | A-22 |
| Use Xmodem to copy a configuration from a serially connected host to a config file. | A-22 |
| Use Xmodem to copy a config file to a serially connected host. | A-23 |

Using the CLI commands described in this section, you can copy switch configurations to and from a switch.

**Note**

For greater security, you can perform all TFTP operations using SFTP as described in the section on *Using Secure Copy and SFTP* on page A-6.

The **include-credentials** command can also be used to save passwords, secret keys, and other security credentials in the running config file. For more information, see the section on "Saving Security Credentials in a Config File" in the *Access Security Guide* for your switch.

## TFTP: Copying a Configuration File to a Remote Host

***Syntax:*** copy < startup-config | running-config > tftp < *ip-addr* > < *remote-file* > [ pc | unix ]
copy config < *filename* > tftp < *ip-addr* > < *remote-file* > [ pc | unix ]

*This command can copy a designated config file in the switch to a TFTP server. For more on multiple configuration files, refer to* Basic Operation Guide.

For example, to upload the current startup configuration to a file named **sw8200** in the configs directory on drive "**d**" in a TFTP server having an IP address of 10.28.227.105:

```
HP Switch# copy startup-config tftp 10.28.227.105
           d:\configs\sw8200
```

## TFTP: Copying a Configuration File from a Remote Host

***Syntax:*** copy tftp < startup-config | running-config > < *ip-address* > < *remote-file* > [ pc | unix ]
copy tftp config < *filename* > < *ip-address* > < *remote-file* > [ pc | unix ]

*This command can copy a configuration from a remote host to a designated config file in the switch. For more on multiple configuration files, refer to* Basic Operation Guide.

*(Refer to* Basic Operation Guide *for more on flash image use.)*

For example, to download a configuration file named **sw8200** in the **configs** directory on drive "**d**" in a remote host having an IP address of 10.28.227.105:

```
HP Switch# copy tftp startup-config 10.28.227.105
           d:\configs\sw8200
```

## TFTP: Copying a Customized Command File to a Switch

Using the **copy tftp** command with the **show-tech** option provides the ability to copy a customized command file to the switch. When the **show tech custom** command is executed, the commands in the custom file are executed instead of the hard-coded list of commands. If no custom file is found, the current hard-coded list is executed. This list contains commands to display data such as the image stamp, running configuration, boot history, port settings, and so on.

***Syntax:*** copy tftp show-tech <ipv4 or ipv6 address> <filename>

*Copy a customized command file to the switch.*

```
HP Switch(config)# copy tftp show-tech 10.10.10.3 commandfile1
```

**Figure A-9. Example of Using the copy tftp show-tech Command to Upload a Customized Command File**

***Syntax:*** show tech custom

*Executes the commands found in a custom file instead of the hard-coded list.*
***Note****: Exit the global config mode (if needed) before executing* **show tech** *commands.*

You can include **show tech** commands in the custom file, with the exception of **show tech custom**. For example, you can include the command **show tech all**.

If no custom file is found, a message displays stating "No SHOW-TECH file found."

```
HP Switch# show tech custom
No SHOW-TECH file found.
```

No custom file was uploaded with the **copy tftp show-tech** command

**Figure A-10. Example of the show tech custom Command**

## Xmodem: Copying a Configuration File to a Serially Connected PC or UNIX Workstation

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation. You will need to:

- Determine a filename to use.
- Know the directory path you will use to store the configuration file.

***Syntax:*** copy < startup-config | running-config > xmodem < pc | unix >
copy config < *filename* > xmodem < pc | unix >

*Uses Xmodem to copy a designated configuration file from the switch to a PC or Unix workstation. For more on multiple configuration files, refer to* Basic Operation Guide.

For example, to copy a configuration file to a PC serially connected to the switch:

1. Determine the file name and directory location on the PC.
2. Execute the following command:
```
HP Switch# copy startup-config xmodem pc
Press 'Enter' and start, XMODEM on your host...
```
3. After you see the above prompt, press **[Enter]**.
4. Execute the terminal emulator commands to begin the file transfer.

## Xmodem: Copying a Configuration File from a Serially Connected PC or UNIX Workstation

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation on which is stored the configuration file you want to copy. To complete the copying, you will need to know the name of the file to copy and the drive and directory location of the file.

***Syntax:*** copy xmodem startup-config < pc | unix >
copy xmodem config < *filename* > < pc | unix >

*Copies a configuration file from a serially connected PC or UNIX workstation to a designated configuration file on the switch. For more on multiple configuration files, refer to* Basic Operation Guide.

For example, to copy a configuration file from a PC serially connected to the switch:

1. Execute the following command:
```
HP Switch# copy xmodem startup-config pc
Device will be rebooted, do you want to continue [y/n]? Y
Press 'Enter' and start XMODEM on your host...
```
2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.
4. When the download finishes, you must reboot the switch to implement the newly downloaded software. Use one of the following commands:

***Syntax:*** boot system flash [ primary | secondary ]
boot system flash [ config < *filename* >]

*Switches boot from the designated configuration file. For more on multiple configuration files, refer to* Basic Operation Guide.

***Syntax:*** reload

*Reboots from the flash image currently in use.*

(For more on these commands, refer to *Basic Operation Guide*.)

# Copying Diagnostic Data to a Remote Host, PC or UNIX Workstation

You can use the CLI to copy the following types of switch data to a text file in a destination device:

- Command Output: Sends the output of a switch CLI command as a file on the destination device.
- Event Log: Copies the switch's Event Log into a file on the destination device.
- Crash Data: software-specific data useful for determining the reason for a system crash.
- Crash Log: Processor-Specific operating data useful for determining the reason for a system crash.

The destination device and copy method options are as follows (CLI key word is in bold):

- Remote Host via **TFTP**.
- Serially connected PC or UNIX workstation via **Xmodem**.

## Copying Command Output to a Destination Device

***Syntax:*** copy command-output < "*cli-command*" > tftp < *ip-address* > < *filepath-filename* >

copy command-output <"*cli-command*"> xmodem

*These commands direct the displayed output of a CLI command to a remote host or to a serially connected PC or UNIX workstation.*

For example, to use Xmodem to copy the output of **show config** to a serially connected PC:

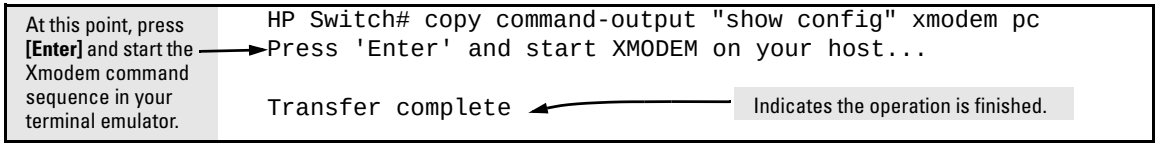



**Figure A-11. Example of Sending Command Output to a File on an Attached PC**

**Note** The command you specify must be enclosed in double-quote marks.

## Copying Event Log Output to a Destination Device

***Syntax:*** copy event-log tftp < *ip-address* > < *filepath_filename* >

copy event-log xmodem <*filename*>

*These commands copy the Event Log content to a remote host or to a serially connected PC or UNIX workstation.*

For example, to copy the event log to a PC connected to the switch:

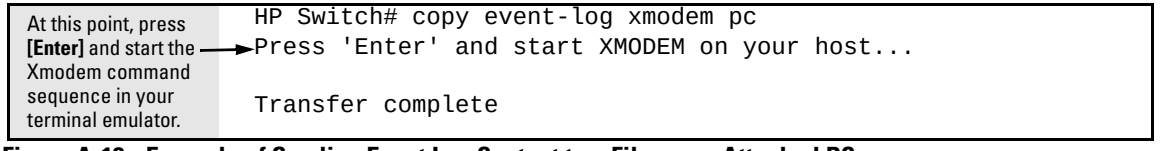



**Figure A-12. Example of Sending Event Log Content to a File on an Attached PC**

## Copying Crash Data Content to a Destination Device

This command uses TFTP or Xmodem to copy the Crash Data content to a destination device.

***Syntax:*** copy crash-data tftp <*ip-address*> <*filename*>

copy crash-data xmodem

*These commands copy the crash data content to a remote host or to a serially connected PC or UNIX workstation.*

For example, to copy the switch's crash data to a file in a PC:

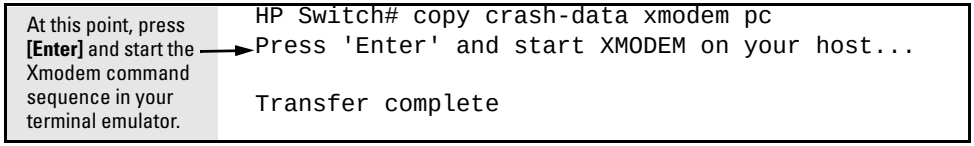



**Figure A-13.Example of Copying Switch Crash Data Content to a PC**

## Copying Crash Log Data Content to a Destination Device

***Syntax:*** copy crash-log tftp <*ip-address*>
copy crash-log xmodem

*These commands copy the Crash Log content to a remote host or to a serially connected PC or UNIX workstation.*

# Monitoring and Analyzing Switch Operation

The switches covered in this guide have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operation:

- **Status:** Includes options for displaying general switch information, management address data, port status, port and trunk group statistics, MAC addresses detected on each port or VLAN, and STP, IGMP, and VLAN data *(page B-1)*.
- **Counters:** Display details of traffic volume on individual ports (page B-7).
- **Event Log**: Lists switch operating events *(*"Using the Event Log for Troubleshooting Switch Problems" on page C-17*)*.
- **Alert Log:** Lists network occurrences detected by the switch—in the Status | Overview screen of the web browser interface *(Getting Started Guide)*.
- **Configurable trap receivers:** Uses SNMP to enable management stations on your network to receive SNMP traps from the switch. (Refer to "SNMP Management Features" on page 5-2.)
- **Port monitoring (mirroring):** Copy all traffic from the specified ports to a designated monitoring port (page B-17).
- **Chassis Locator LED:** The blue Locator LED lights up when you enter the **chassislocate** command (

**Note**

Link test and ping test—analysis tools in troubleshooting situations—are described in appendix C, "Troubleshooting". Refer to "Diagnostic Tools" on page C-44.

## Status and Counters Data

This section describes the status and counters screens available through the switch console interface and/or the web browser interface.

**Note**

You can access all console screens from the web browser interface via Telnet to the console. Telnet access to the switch is available in the Device View window under the **Configuration** tab.

| Status or Counters Type | Interface | Purpose | Page |
|---|---|---|---|
| Menu Access to Status and Counters | Menu | Access menu interface for status and counter data. | **B-2** |
| General System Information | Menu, CLI | Lists switch-level operating information. | **B-3** |
| Management Address Information | Menu, CLI | Lists the MAC address, IP address, and IPX network number for each VLAN or, if no VLANs are configured, for the switch. | **B-5** |
| Port Status | Menu, CLI, Web | Displays the operational status of each port. | **B-6** |
| Port and Trunk Statistics and Flow Control Status | Menu, CLI, Web | Summarizes port activity and lists per-port flow control status. | **B-7** |
| VLAN Address Table | Menu, CLI | Lists the MAC addresses of nodes the switch has detected on specific VLANs, with the corresponding switch port. | **B-9** |
| Port Address Table | Menu, CLI | Lists the MAC addresses that the switch has learned from the selected port. | **B-9** |
| STP Information | Menu, CLI | Lists Spanning Tree Protocol data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis. | **B-13** |
| IGMP Status | Menu, CLI | Lists IGMP groups, reports, queries, and port on which querier is located. | **B-15** |
| VLAN Information | Menu, CLI | For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status. | **B-15** |
| Port Status Overview and Port Counters | Web | Shows port utilization and counters, and the Alert Log. | **B-17** |

# Menu Access To Status and Counters

At the Main Menu, display the Status and Counters menu by selecting:

**1. Status and Counters**

```
  1. General System Information
  2. Switch Management Address Information
  3. Module Information
  4. Port Status
  5. Port Counters
  6. Vlan Address Table
  7. Port Address Table
  8. Spanning Tree Information
  0. Return to Main Menu...

Displays switch management information including software versions.
To select menu item, press item number, or highlight item and press <Enter>.
```

**Figure B-1. The Status and Counters Menu**

Each of the above menu items accesses the read-only screens described on the following pages. Refer to the online help for a description of the entries displayed in these screens.

# General System Information

## Menu Access

From the console Main Menu, select:

**1. Status and Counters**

**1. General System Information**

```
============================- TELNET - MANAGER MODE -=========================
                Status and Counters - General System Information

  System Contact     :George
  System Location    :Buiding A

  Software revision  : YA.15.XX          Base MAC Addr      : 001c2e-95b900
  ROM Version        : YA.15.01          Serial Number      : SG862II056

  Up Time            : 46 hours         Memory   - Total   :
  CPU Util (%)       : 19                          Free    :

  IP Mgmt  - Pkts Rx : 532,398          Packet   - Total   : 6750
             Pkts Tx : 3005             Buffers    Free    : 5093
                                                   Lowest  : 5030
                                                   Missed  : 0
 Actions->   Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure B-2. Example of General Switch Information**

This screen dynamically indicates how individual switch resources are being used. Refer to the online Help for details.

## CLI Access to System Information

The **show system** command displays general system information about the switch.

***Syntax:*** show system [information] ]

*Displays global system information and operational parameters for the switch.*

***Syntax:*** show system [information] ]

information

*Displays global system information and operational parameters for the switch.*

```
HP Switch(config)# show system information
 Status and Counters - General System Information

  System Name        : Switch
  System Contact     :
  System Location    :

  MAC Age Time (sec) : 300

  Time Zone          : 0
  Daylight Time Rule : None


  Software revision  : YA.15.XX          Base MAC Addr      : 001635-b57cc0
  ROM Version        : YA.15.01          Serial Number      : LP621KI005

  Up Time            : 10 days          Memory   - Total   : 152,455,616
  CPU Util (%)       : 3                           Free    : 110,527,264

  IP Mgmt  - Pkts Rx : 6,000,531              Packet   - Total   : 6750
             Pkts Tx : 10,133                 Buffers    Free    : 5086
                                                         Lowest  : 5086
                                                         Missed  : 0
```

**Figure B-3. Example of Switch System Information**

## Task Monitor—Collecting Processor Data

The task monitor feature allows you to enable or disable the collection of processor utilization data. The **task-monitor cpu** command is equivalent to the existing debug mode command "**taskusage -d**". (The **taskUsageShow** command is available as well.)

When the **task-monitor** command is enabled, the **show cpu** command summarizes the processor usage by protocol and system functions.

***Syntax:*** [no] task-monitor cpu

*Allows the collection of processor utilization data. Only manager logins can execute this command. The settings are not persistent, that is, there are no changes to the configuration.*
*Default: Disabled*

```
HP Switch(config)# task-monitor cpu
HP Switch(config)# show cpu

2 percent busy, from 2865 sec ago
1 sec ave: 9 percent busy
5 sec ave: 9 percent busy
1 min ave: 1 percent busy

 % CPU | Description
-------+---------------------------
    99 | Idle
```

**Figure B-4. Example of the task-monitor cpu Command and show cpu Output**

# Switch Management Address Information

## Menu Access

From the Main Menu, select:

**1 Status and Counters …**

**2. Switch Management Address Information**

```
==========================- CONSOLE - MANAGER MODE -============================
              Status and Counters - Management Address Information

  Time Server Address : Disabled

   VLAN Name    MAC Address          IP Address
  ------------  -------------------  -------------------
  DEFAULT_VLAN  0001e7-a09900        10.28.227.101
  VLAN-22       0001e7-a09900        Disabled
  VLAN-33       0001e7-a09900        Disabled


 Actions->   Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure B-5. Example of Management Address Information with VLANs Configured**

This screen displays addresses that are important for management of the switch. If multiple VLANs are *not* configured, this screen displays a single IP address for the entire switch. Refer to the online Help for details.

**Note**

As shown in figure B-5, all VLANs on the switches use the same MAC address. (This includes both the statically configured VLANs and any dynamic VLANs existing on the switch as a result of GVRP operation.)

Also, the switches covered in this guide use a multiple forwarding database. When using multiple VLANs and connecting a switch to a device that uses a single forwarding database, such as a Switch 4000M, there are cabling and tagged port VLAN requirements. For more on this topic, refer to the section titled “Multiple VLAN Considerations” in the “Static Virtual LANs (VLANs) chapter of the *Advanced Traffic Management Guide* for your switch.

### CLI Access

***Syntax:*** show management

## Port Status

The web browser interface and the console interface show the same port status data.

### Menu: Displaying Port Status

From the Main Menu, select:

**1. Status and Counters …**
**4. Port Status**

```
                    Status and Counters - Port Status

                  Intrusion                                Flow
 Port     Type       Alert    Enabled  Status     Mode      Ctrl
 -----  ---------  ---------  -------  ------  ----------  -----
  1                No         Yes      Down                off
  2                No         Yes      Down                off
  3                No         Yes      Down                off
  4                No         Yes      Down                off
  5     10/100TX   No         Yes      Up      100FDx      off
  6     10/100TX   No         Yes      Down    10FDx       off
  7     10/100TX   No         Yes      Down    10FDx       off
  8     10/100TX   No         Yes      Down    10FDx       off
  9     10/100TX   No         Yes      Down    10FDx       off
  10    10/100TX   No         Yes      Down    10FDx       off
  11    10/100TX   No         Yes      Down    10FDx       off

 Actions->   Back     Intrusion log     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure B-6. Example of Port Status on the Menu Interface**

### CLI Access

***Syntax:*** show interfaces brief

### Web Access

1. Click on the **Status** tab.
2. Click on **[Port Status]**.

## Viewing Port and Trunk Group Statistics and Flow Control Status

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing port and trunk statistics for all ports, and flow control status | n/a | page B-8 | page B-9 | page B-9 |
| viewing a detailed summary for a particular port or trunk | n/a | page B-8 | page B-9 | page B-9 |
| resetting counters | n/a | page B-8 | page B-9 | page B-9 |

These features enable you to determine the traffic patterns for each port since the last reboot or reset of the switch. You can display:

- A general report of traffic on all LAN ports and trunk groups in the switch, along with the per-port flow control status (On or Off).
- A detailed summary of traffic on a selected port or trunk group.

You can also reset the counters for a specific port.

The menu interface and the web browser interface provide a dynamic display of counters summarizing the traffic on each port. The CLI lets you see a static "snapshot" of port or trunk group statistics at a particular moment.

As mentioned above, rebooting or resetting the switch resets the counters to zero. You can also reset the counters to zero for the current session. This is useful for troubleshooting. Refer to the "Note On Reset", below.

**Note on Reset**

The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Thus, using the **Reset** action resets the displayed counters to zero for the current session only. Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

## Menu Access to Port and Trunk Statistics

To access this screen from the Main Menu, select:

**1. Status and Counters …**

**4. Port Counters**

```
=========================- CONSOLE - MANAGER MODE -============================
                    Status and Counters - Port Counters

                                                                        Flow
  Port     Total Bytes   Total Frames     Errors Rx      Drops Tx      Ctrl
 -------  -------------  -------------  -------------  -------------  ------
  1            195,072            323              0              0  off
  2            651,816            871              0              0  off
  3-Trk1       290,163            500              0              0  off
  4-Trk1       260,134            501              0              0  off
  5            859,363           5147              0              0  off
  6            674,574           1693              0              0  off
  7             26,554            246              0              0  off
  8            113,184            276              0              0  off

 Actions->   Back     Show details     Reset     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure B-7. Example of Port Counters on the Menu Interface**

To view details about the traffic on a particular port, use the ↓ key to highlight that port number, then select **Show Details**. For example, selecting port 2 displays a screen similar to figure B-8, below.

```
=========================- CONSOLE - MANAGER MODE -============================
                Status and Counters - Port Counters - Port 2

  Link Status     : Up

  Bytes Rx        : 630,746            Bytes Tx        : 21,070
  Unicast Rx      : 568                Unicast Tx      : 285
  Bcast/Mcast Rx  : 18                 Bcast/Mcast Tx  : 0

  FCS Rx          : 0                  Drops Tx        : 0
  Alignment Rx    : 0                  Collisions Tx   : 0
  Runts Rx        : 0                  Late Colln Tx   : 0
  Giants Rx       : 0                  Excessive Colln : 0
  Total Rx Errors : 0                  Deferred Tx     : 0

 Actions->   Back     Reset     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

**Figure B-8. Example of the Display for Show details on a Selected Port**

This screen also includes the **Reset** action for the current session. (Refer to the “Note on Reset” on page B-7.)

### CLI Access To Port and Trunk Group Statistics

**To Display the Port Counter Summary Report.**

***Syntax:*** show interfaces

*This command provides an overview of port activity for all ports on the switch.*

**To Display a Detailed Traffic Summary for Specific Ports.**

***Syntax:*** show interfaces < *port-list* >

*This command provides traffic details for the port(s) you specify*

**To Reset the Port Counters for a Specific Port.**

***Syntax:*** clear statistics < *port-list* >

*This command resets the counters for the specified ports to zero for the current session. (See the "Note on Reset" on page B-7.)*

### Web Browser Access To View Port and Trunk Group Statistics

1. Click on the **Status** tab.
2. Click on **[Port Counters].**
3. To refresh the counters for a specific port, click anywhere in the row for that port, then click on **[Refresh].**

**Note**

To reset the port counters to zero, you must reboot the switch.

## Viewing the Switch's MAC Address Tables

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| viewing MAC addresses on all ports on a specific VLAN | n/a | page B-10 | page B-12 | — |
| viewing MAC addresses on a specific port | n/a | page B-11 | page B-12 | — |
| searching for a MAC address | n/a | page B-11 | page B-12 | — |

These features help you to view:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

## Menu Access to the MAC Address Views and Searches

**Per-VLAN MAC-Address Viewing and Searching.** This feature lets you determine which switch port on a selected VLAN is being used to communicate with a specific device on the network. The per-VLAN listing includes:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

1. From the Main Menu, select:

   **1. Status and Counters**
   **5. VLAN Address Table**

2. The switch then prompts you to select a VLAN.

```
Select VLAN : DEFAULT_VLAN
```

3. Use the Space bar to select the VLAN you want, then press **[Enter]**. The switch then displays the MAC address table for that VLAN:

```
============================- CONSOLE - MANAGER MODE -=============================
                        Status and Counters - Address Table

   MAC Address   Located on Port
  -------------  ---------------
  0030c1-7f49c0   3
  0030c1-7fec40   1
  0030c1-b29ac0   3
  0060b0-17de5b   3
  0060b0-880a80   2
  0060b0-df1a00   3
  0060b0-df2a00   3
  0060b0-e9a200   3
  009027-e74f90   3
  080009-21ae84   3
  080009-62c411   3
  080009-6563e2   3

 Actions->   Back     Search     Next page     Prev page     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure B-9. Example of the Address Table**

To page through the listing, use **Next page** and **Prev page**.

**Finding the Port Connection for a Specific Device on a VLAN.** This feature uses a device's MAC address that you enter to identify the port used by that device.

1. Proceeding from figure B-9, press **[S]** (for **Search**), to display the following prompt:

   ```
   Enter MAC address: _
   ```

2. Type the MAC address you want to locate and press **[Enter]**. The address and port number are highlighted if found. If the switch does not find the MAC address on the currently selected VLAN, it leaves the MAC address listing empty.

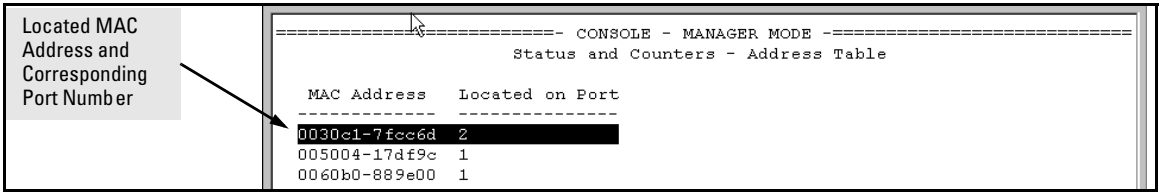



**Figure B-10. Example of Menu Indicating Located MAC Address**

3. Press **[P]** (for **Prev page**) to return to the full address table listing.

**Port-Level MAC Address Viewing and Searching.** This feature displays and searches for MAC addresses on the specified port instead of for all ports on the switch.

1. From the Main Menu, select:

   **1. Status and Counters**
   **7. Port Address Table**

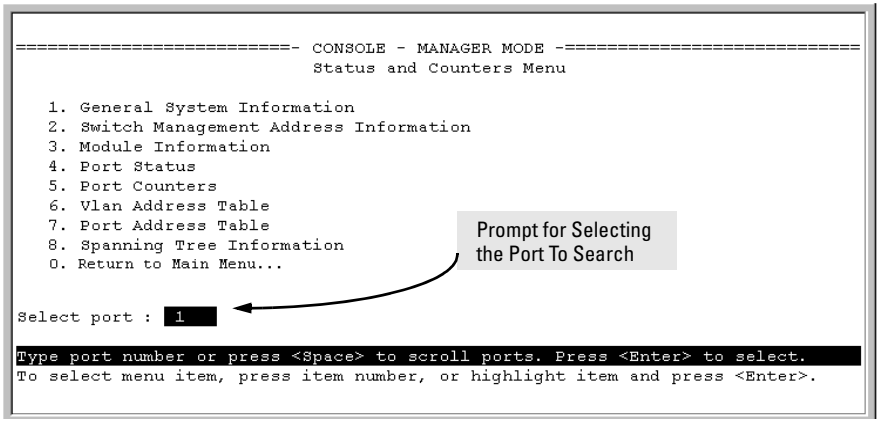



**Figure B-11. Listing MAC Addresses for a Specific Port**

2. Use the Space bar to select the port you want to list or search for MAC addresses, then press **[Enter]** to list the MAC addresses detected on that port.

**Determining Whether a Specific Device Is Connected to the Selected Port.** Proceeding from step 2, above:

1. Press **[S]** (for **Search**), to display the following prompt:

   ```
   Enter MAC address: _
   ```

2. Type the MAC address you want to locate and press **[Enter]**. The address is highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.
3. Press **[P]** (for **Prev page**) to return to the previous per-port listing.

## CLI Access for MAC Address Views and Searches

***Syntax:*** show mac-address
[ vlan < *vlan-id* >]
[< *port-list* >]
[< mac-addr >]

**To List All Learned MAC Addresses on the Switch, with The Port Number on Which Each MAC Address Was Learned.**

```
HP Switch> show mac-address
```

**To List All Learned MAC Addresses on one or more ports, with Their Corresponding Port Numbers.** For example, to list the learned MAC address on ports 1 through 4 and port 6:

```
HP Switch> show mac-address 1-4,6
```

**To List All Learned MAC Addresses on a VLAN, with Their Port Numbers.** This command lists the MAC addresses associated with the ports for a given VLAN. For example:

```
HP Switch> show mac-address vlan 100
```

**Note**

The switches covered in this guide operate with a multiple forwarding database architecture.

**To Find the Port On Which the Switch Learned a Specific MAC**

**Address.** For example, to find the port on which the switch learns a MAC address of 080009-21ae84:

```
HP Switch# show mac-address 080009-21ae84
 Status and Counters - Address Table - 080009-21ae84
  MAC Address : 080009-21ae34
  Located on Port : 2
```

# Spanning Tree Protocol (MSTP) Information

## CLI Access to MSTP Data

This option lists the MSTP configuration, root data, and per-port data (cost, priority, state, and designated bridge).

***Syntax:*** show spanning-tree

*This command displays the switch's global and regional spanning-tree status, plus the per-port spanning-tree operation at the regional level. Note that values for the following parameters appear only for ports connected to active devices:* **Designated Bridge**, **Hello Time**, **PtP**, *and* **Edge**.

```
HP Switch(config)# show spanning-tree
 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1,66

  Switch MAC Address : 0004ea-5e2000
  Switch Priority    : 32768
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 0
  Time Since Last Change : 2 hours

  CST Root MAC Address : 00022d-47367f
  CST Root Priority    : 0
  CST Root Path Cost   : 4000000
  CST Root Port        : 1

  IST Regional Root MAC Address : 000883-028300
  IST Regional Root Priority    : 32678
  IST Regional Root Path Cost   : 200000
  IST Remaining Hops            : 19

                 |            Prio             | Designated    Hello
  Port Type      | Cost       rity  State      | Bridge        Time  PtP Edge
  ---- --------- + ---------- ----- ---------- + ------------- ----- --- ----
  1    10/100TX  | Auto       128   Forwarding | 000883-028300 9     Yes No
  2    10/100TX  | Auto       128   Blocking   | 0001e7-948300 9     Yes No
  3    10/100TX  | Auto       128   Forwarding | 000883-02a700 2     Yes No
  4    10/100TX  | Auto       128   Disabled   |
  5    10/100TX  | Auto       128   Disabled   |
  .       .          .         .       .
```

**Figure B-12. Output from show spanning-tree Command**

## Internet Group Management Protocol (IGMP) Status

Use the CLI to display the following IGMP status on a per-VLAN basis:

| Show Command | Output |
|---|---|
| show ip igmp | Global command listing IGMP status for all VLANs configured in the switch:<br>• VLAN ID (VID) and name<br>• Active group addresses per VLAN<br>• Number of report and query packets per group<br>• Querier access port per VLAN |
| show ip igmp <*vlan-id*> | Per-VLAN command listing above IGMP status for specified VLAN (VID) |
| show ip igmp group <*ip-addr*> | Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data. |

For example, suppose that **show ip igmp** listed an IGMP group address of 224.0.1.22. You could get additional data on that group by executing the following:

```
HP Switch> show ip igmp group 224.0.1.22

 IGMP ports for group 224.0.1.22
  Port Type      Access      Age Timer Leave Timer
  ---- --------- ----------- --------- -----------
  3    10/100TX  host        0         0
```

**Figure B-13. Example of IGMP Group Data**

## VLAN Information

The switch uses the CLI to display the following VLAN status:

| Show Command | Output |
|---|---|
| show vlan | Lists:<br>• Maximum number of VLANs to support<br>• Existing VLANs<br>• Status (static or dynamic)<br>• Primary VLAN |
| show vlan <*vlan-id*> | For the specified VLAN, lists:<br>• Name, VID, and status (static/dynamic)<br>• Per-Port mode (tagged, untagged, forbid, no/auto)<br>• "Unknown VLAN" setting (Learn, Block, Disable)<br>• Port status (up/down) |

For example, suppose that your switch has the following VLANs:

| Ports | VLAN | VLANID |
|---|---|---|
| 1-12 | DEFAULT_VLAN | 1 |
| 13-14 | VLAN-33 | 33 |
| 15-20 | VLAN-44 | 44 |

The next three figures show how you could list data on the above VLANs.

```
HP Switch> show vlan
 Status and Counters - VLAN Information
  Maximum VLANs to support : 256
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :
  VLAN ID Name                 Status       Voice Jumbo
  ------- -------------------- ------------ ----- -----
  1       DEFAULT_VLAN         Port-based   No    No
  33      VLAN-33              Static       No    No
  44      VLAN-44              Static       No    No
```

**Figure B-14. Example of VLAN Listing for the Entire Switch**

Because ports 2 and 3 are not members of VLAN-44, it does not appear in this listing.

```
HP Switch>show vlan ports 1-2
 Status and Counters - VLAN Information - for ports 1,2
  VLAN ID        Name         Status
  -------------- ------------ ---------
  1              DEFAULT_VLAN Static
  33             VLAN-33      Static
```

**Figure B-15. Example of VLAN Listing for Specific Ports**

```
HP Switch(config)# show vlan 1
 Status and Counters - VLAN Information - VLAN 1
  VLAN ID : 1
  Name : DEFAULT_VLAN
  Status : Port-based  Voice : No
  Jumbo : No
  Port Information Mode     Unknown VLAN Status
  --------------- -------- ------------ ----------
  1               Untagged Learn        Up
  2               Tagged   Learn        Up
  3               Untagged Learn        Up
  4               Untagged Learn        Down
```

**Figure B-16. Example of Port Listing for an Individual VLAN**

## Web Browser Interface Status Information

The “home” screen for the web browser interface is the Status Overview screen, as shown below. As the title implies, it provides an overview of the status of the switch, including summary graphs indicating the network utilization on each of the switch ports, symbolic port status indicators, and the Alert Log, which informs you of any problems that may have occurred on the switch.

For more information on this screen, refer to Getting Started Guide.

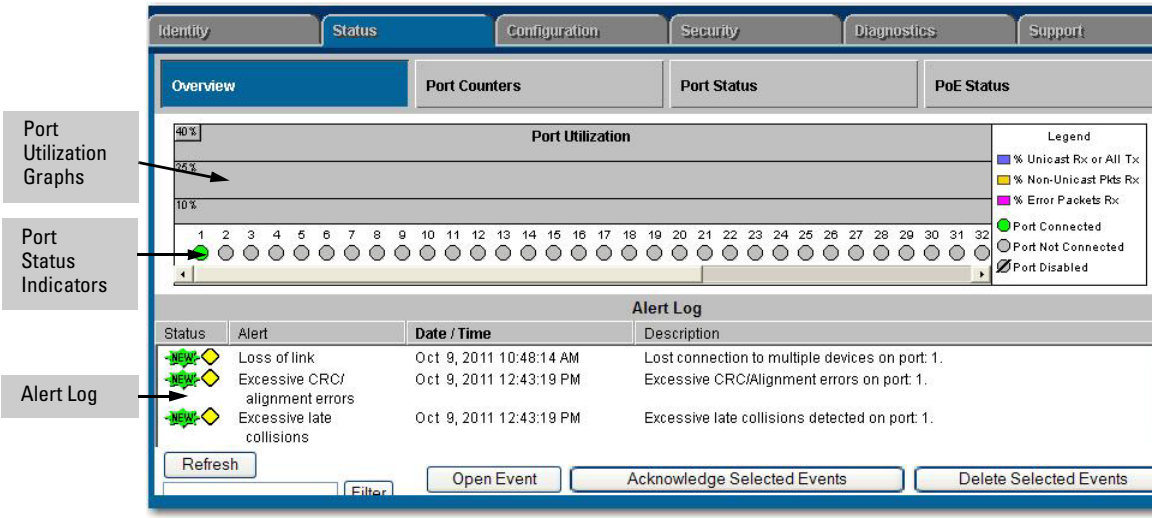



**Figure B-17. Example of a Web Browser Interface Status Overview Screen**

# Interface Monitoring Features

**Port Monitoring Features**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| display monitoring configuration | disabled | page B-18 | page B-20 | page B-21 |
| configure the monitor port(s) | ports: none | page B-18 | page B-20 | page B-21 |
| selecting or removing ports | none selected | page B-18 | page B-21 | page B-21 |

You can designate monitoring of inbound and outbound traffic on ports and static trunks. The switch monitors network activity by copying all traffic inbound and outbound on the specified interfaces to the designated monitoring port, to which a network analyzer can be attached.

If a tagged packet arrives on a monitored port, the packet will remain tagged when it goes out a monitored port even if that port is configured as untagged. If the packet is untagged, it will remain untagged going out the monitor port. The monitor port state (tagged or untagged) does not affect the tagging of the packet. However, egress mirroring does not reflect the tagged or untagged characteristic to the mirror port, instead it reflects the tagged or untagged characteristic of the mirror port.

**Note** When both inbound and outbound monitoring is done, and IGMP is enabled on any VLAN, you may get two copies of IGMP packets on the monitored port.

**Note** VLANs and port trunks cannot be used as a monitoring port.

The switch can monitor static LACP trunks, but not dynamic LACP trunks.

It is possible, when monitoring multiple interfaces in networks with high traffic levels, to copy more traffic to a monitor port than the link can support. In this case, some packets may not be copied to the monitor port.

## Menu: Configuring Port and Static Trunk Monitoring

This procedure describes configuring the switch for monitoring when monitoring is disabled. (If monitoring has already been enabled, the screens will appear differently than shown in this procedure.)

1. From the Console Main Menu, Select:

   **2. Switch Configuration...**

   **3. Network Monitoring Port**

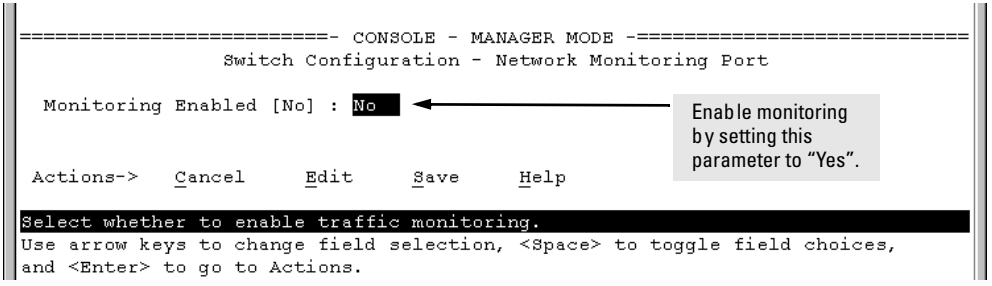
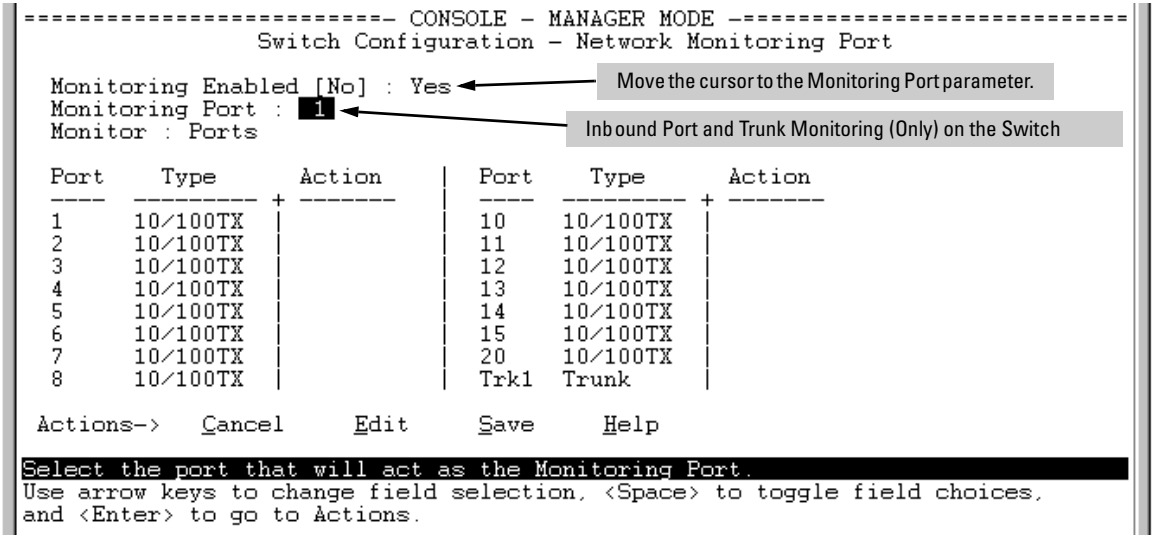



**Figure B-18. The Default Network Monitoring Configuration Screen**

2. In the Actions menu, press **[E]** (for `Edit`).
3. If monitoring is currently disabled (the default) then enable it by pressing the Space bar (or **[Y]**) to select `Yes`.
4. Press the down arrow key to display a screen similar to the following and move the cursor to the **Monitoring Port** parameter.




```
============================= CONSOLE - MANAGER MODE ==============================
                  Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port : 1
  Monitor : Ports

  Port    Type       Action     |  Port    Type       Action
  ----  ---------- + -------    |  ----  ---------- + -------
  1     10/100TX   |            |  10    10/100TX   |
  2     10/100TX   |            |  11    10/100TX   |
  3     10/100TX   |            |  12    10/100TX   |
  4     10/100TX   |            |  13    10/100TX   |
  5     10/100TX   |            |  14    10/100TX   |
  6     10/100TX   |            |  15    10/100TX   |
  7     10/100TX   |            |  20    10/100TX   |
  8     10/100TX   |            |  Trk1  Trunk      |

 Actions->   Cancel     Edit     Save     Help

Select the port that will act as the Monitoring Port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure B-19. How To Select a Monitoring Port**

5. Use the Space bar to select the port to use for monitoring.
6. Use the down arrow key to move the cursor to the **Action** column for the individual ports and position the cursor at a port you want to monitor.
7. Press the Space bar to select **Monitor** for each port and trunk that you want monitored. (Use the down arrow key to move from one interface to the next in the **Action** column.)
8. When you finish selecting ports to monitor, press **[Enter]**, then press **[S]** (for **Save**) to save your changes and exit from the screen.
9. Return to the Main Menu.

## CLI: Configuring Port and Static Trunk Monitoring

**Port and Static Trunk Monitoring Commands Used in This Section**

| | |
|---|---|
| show monitor | below |
| mirror-port | page B-20 |
| monitor | page B-21 |

You must use the following configuration sequence to configure port and static trunk monitoring in the CLI:

1. Assign a monitoring (mirror) port.
2. Designate the port(s) and/or static trunk(s) to monitor.

**Displaying the Monitoring Configuration.**

***Syntax:*** show monitor

*This command lists the port assigned to receive monitored traffic and the ports and/or trunks being monitored.*

For example, if you assign port 6 as the monitoring port and configure the switch to monitor ports 1 - 3, **show monitor** displays the following:

```
HP Switch(config)# show monitor

 Network Monitoring Port
  Mirror Port: 4

  Monitoring sources
  ------------------
  1
  2
  3
```

Port receiving monitored traffic.

Monitored Ports

**Figure B-20. Example of Monitored Port Listing**

**Configuring the Monitor Port.**

***Syntax:*** [no] mirror-port [< *port-num* >]

*This command assigns or removes a monitoring port, and must be executed from the global configuration level. Removing the monitor port disables port monitoring and resets the monitoring parameters to their factory-default settings.*

For example, to assign port 6 as the monitoring port:

```
HP Switch(config)# mirror-port 6
```

To turn off monitoring:

```
HP Switch(config)# no mirror-port
```

**Selecting or Removing Monitoring Source Interfaces.** After you configure a monitor port you can use either the global configuration level or the interface context level to select ports or static trunks as monitoring sources. You can also use either level to remove monitoring sources.

***Syntax:*** [no] interface < *monitor-list* > monitor

*where:*

*< monitor-list > Includes port numbers and static trunk names such as **4**,**7**, **5-8**, **trk1**.*
*Identifies the switch elements to monitor through the currently configured monitor port. You can monitor the port(s) and static trunk(s) available on the switch.*

Elements in the monitor list can include port numbers and static trunk names at the same time.

For example, with a port such as port 6 configured as the monitoring (mirror) port, you would use either of the following commands to select these interfaces for monitoring:

- 1 through 3, and 5
- Trunk 2

```
HP Switch(config)# int 1-3, 5, trk2, monitor
```

**Figure B-21. Examples of Selecting Ports and Static Trunks as Monitoring Sources**

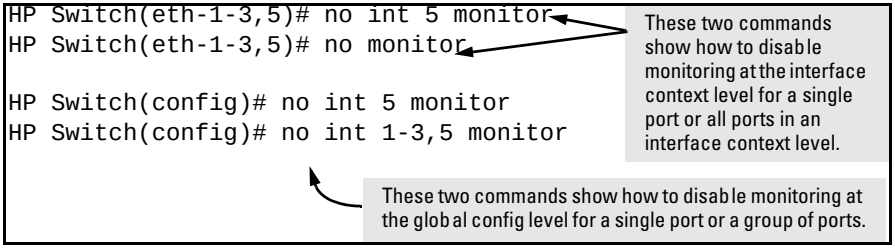



**Figure B-22. Examples of Removing Ports as Monitoring Sources**

## Web: Configuring Port Monitoring

To enable port monitoring:

1. Click on the **Configuration** tab.
2. Click on **[Monitor Port].**

3. To monitor one or more ports.
   a. Click on the radio button for **Monitor Selected Ports**.
   b. Select the port(s) to monitor.
4. Click on **[Apply Changes]**.

To remove port monitoring:

1. Click on the **[Monitoring Off]** radio button.
2. Click on **[Apply Changes]**.

For web-based Help on how to use the web browser interface screen, click on the **[?]** button provided on the web browser screen.

# Locating a Device

If you are trying to locate a particular switch you can enter the **chassislocate** command. The blue Locator LED will light up on that switch.

***Syntax:*** chassislocate [ blink | on | off ]

*Locate a device by using the blue Locate LED on the front panel.*

blink <1-1440>

*Blinks the chassis Locate LED for a selected number of minutes (default is 30 minutes).*

on <1-1440>

*Turns the chassis Locate LED on for a selected number of minutes (default is 30 minutes).*

off

*Turns the chassis Locate LED off.*

```
HP Switch(config)# chassislocate
 blink <1-1440>        Blink the chassis locate led (default 30 minutes).
 off                   Turn the chassis locate led off.
 on <1-1440>           Turn the chassis locate led on (default 30 minutes).
HP Switch(config)# chassislocate
```

**Figure B-23. The chassislocate command**

# Troubleshooting

This appendix addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the *Installation Guide* you received with the switch.)

**Note**

HP periodically places switch software updates on the HP web site. HP recommends that you check this web site for software updates that may have fixed a problem you are experiencing.

For information on support and warranty provisions, refer to the Support and Warranty booklet shipped with the switch.

## Troubleshooting Approaches

Use these approaches to diagnose switch problems:

- Check the HP web site for software updates that may have solved your problem: **www.hp.com/Networking**
- Check the switch LEDs for indications of proper switch operation:
  - Each switch port has a Link LED that should light whenever an active network device is connected to the port.
  - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs.

    Refer to the *Installation Guide* shipped with the switch for a description of the LED behavior and information on using the LEDs for troubleshooting.
- Check the network topology/installation. Refer to the *Installation Guide* shipped with the switch for topology information.
- Check cables for damage, correct type, and proper connections. You should also use a cable tester to check your cables for compliance to the relevant IEEE 802.3 specification. Refer to the *Installation Guide* shipped with the switch for correct cable types and connector pin-outs.
- Use IMC to help isolate problems and recommend solutions.

- Use the Port Utilization Graph and Alert Log in the web browser interface included in the switch to help isolate problems. Refer to *Getting Started Guide* for operating information. These tools are available through the web browser interface:
  - Port Utilization Graph
  - Alert Log
  - Port Status and Port Counters screens
  - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or Telnet to the switch console. Refer to *Getting Started Guide* for operating information on the Menu and CLI interfaces included in the console. These tools are available through the switch console
  - Status and Counters screens
  - Event Log
  - Diagnostics tools (Link test, Ping test, configuration file browser, and advanced user commands)

# Browser or Telnet Access Problems

**Cannot access the web browser interface:**

- Access may be disabled by the **Web Agent Enabled** parameter in the switch console. Check the setting on this parameter by selecting:

  **2. Switch Configuration ...**

  **1. System Information**
- The switch may not have the correct IP address, subnet mask or gateway. Verify by connecting a console to the switch's Console port and selecting:

  **2. Switch Configuration ...**

  **5. IP Configuration**

  **Note:** If DHCP/Bootp is used to configure the switch, the IP addressing can be verified by selecting:

  **1. Status and Counters ...**

  **2. Switch Management Address Information**

  also check the DHCP/Bootp server configuration to verify correct IP addressing.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows web browser access only to a device having an authorized IP address. For more information on IP Authorized managers, refer to the *Access Security Guide* for your switch.
- Java™ applets may not be running on the web browser. They are required for the switch web browser interface to operate correctly. Refer to the online Help on your web browser for how to run the Java applets.

**Cannot Telnet into the switch console from a station on the network:**

- Telnet access may be disabled by the **Inbound Telnet Enabled** parameter in the System Information screen of the menu interface:

  **2. Switch Configuration**

  **1. System Information**

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

  **2. Switch Configuration**

  **5. IP Configuration**

  **Note:** If DHCP/Bootp is used to configure the switch, refer to the **Note**, above.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, refer to the *Access Security Guide* for your switch.

# Unusual Network Activity

Network activity that fails to meet accepted norms may indicate a hardware problem with one or more of the network components, possibly including the switch. Such problems can also be caused by a network loop or simply too much traffic for the network as it is currently designed and implemented.

Unusual network activity is usually indicated by the LEDs on the front of the switch or measured with the switch console interface or with a network management tool such as IMC. Refer to the *Installation Guide* you received with the switch for information on using LEDs to identify unusual network activity.

A topology loop can also cause excessive network activity. The Event Log "FFI" messages can be indicative of this type of problem.

## General Problems

**The network runs slow; processes fail; users cannot access servers or other devices.** Broadcast storms may be occurring in the network. These may be due to redundant links between nodes.

- If you are configuring a port trunk, finish configuring the ports in the trunk before connecting the related cables. Otherwise you may inadvertently create a number of redundant links (i.e. topology loops) that will cause broadcast storms.
- Turn on Spanning Tree Protocol to block redundant links (i.e. topology loops)
- Check for FFI messages in the Event Log.

**Duplicate IP Addresses.** This is indicated by this Event Log message:

> **ip: Invalid ARP source:** *IP address* **on** *IP address*
>
> *where:* both instances of *IP address* are the same address, indicating the switch's IP address has been duplicated somewhere on the network.

**Duplicate IP Addresses in a DHCP Network.** If you use a DHCP server to assign IP addresses in your network and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server "leases" the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, then is subsequently configured to issue IP addresses that will expire after a limited duration. One solution is to configure "reservations" in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, refer to the documentation for the DHCP server.

One indication of a duplicate IP address in a DHCP network is this Event Log message:

`ip: Invalid ARP source: < `*IP-address*` > on <`*IP-address*`>`

*where:* both instances of *IP-address* are the same address, indicating the IP address that has been duplicated somewhere on the network.

**The Switch Has Been Configured for DHCP/Bootp Operation, But Has Not Received a DHCP or Bootp Reply.** When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

## 802.1Q Prioritization Problems

**Ports configured for non-default prioritization (level 1 - 7) are not performing the specified action.** If the ports were placed in a trunk group after being configured for non-default prioritization, the priority setting was automatically reset to zero (the default). Ports in a trunk group operate only at the default priority setting.

## IGMP-Related Problems

**IP Multicast (IGMP) Traffic That Is Directed By IGMP Does Not Reach IGMP Hosts or a Multicast Router Connected to a Port.** IGMP must be enabled on the switch and the affected port must be configured for "Auto" or "Forward" operation.

**IP Multicast Traffic Floods Out All Ports; IGMP Does Not Appear To Filter Traffic.** The IGMP feature does not operate if the switch or VLAN does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch or VLAN, do either of the following:

- **Try Using the Web Browser Interface:** If you can access the web browser interface, then an IP address is configured.
- **Try To Telnet to the Switch Console:** If you can Telnet to the switch, then an IP address is configured.
- **Using the Switch Console Interface:** From the Main Menu, check the Management Address Information screen by clicking on

**1. Status and Counters**

**2. Switch Management Address Information**

## LACP-Related Problems

Unable to enable LACP on a port with the **interface < *port-number* > lacp** command. In this case, the switch displays the following message:

Operation is not allowed for a trunked port.

You cannot enable LACP on a port while it is configured as static **Trunk** port. To enable LACP on static-trunked port, first use the **no trunk < *port-number* >** command to disable the static trunk assignment, then execute **interface < *port-number* > lacp**.

**Caution**

Removing a port from a trunk without first disabling the port can create a traffic loop that can slow down or halt your network. Before removing a port from a trunk, HPrecommends that you either disable the port or disconnect it from the LAN.

## Port-Based Access Control (802.1X)-Related Problems

**Note**

To list the 802.1X port-access Event Log messages stored on the switch, use **show log 802**.

See also “Radius-Related Problems” on page C-9.

**The switch does not receive a response to RADIUS authentication requests.** In this case, the switch will attempt authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

- Use **ping** to ensure that the switch has access to the configured RADIUS servers.
- Verify that the switch is using the correct encryption key (RADIUS secret key) for each server.
- Verify that the switch has the correct IP address for each RADIUS server.
- Ensure that the **radius-server timeout** period is long enough for network conditions.

**The switch does not authenticate a client even though the RADIUS server is properly configured and providing a response to the authentication request.** If the RADIUS server configuration for authenticating the client includes a VLAN assignment, ensure that the VLAN exists as a static VLAN on the switch. Refer to "How 802.1X Authentication Affects VLAN Operation" in the *Access Security Guide* for your switch.

**During RADIUS-authenticated client sessions, access to a VLAN on the port used for the client sessions is lost.** If the affected VLAN is configured as untagged on the port, it may be temporarily blocked on that port during an 802.1X session. This is because the switch has temporarily assigned another VLAN as untagged on the port to support the client access, as specified in the response from the RADIUS server. Refer to "How 802.1X Authentication Affects VLAN Operation" in the *Access Security Guide* for your switch.

**The switch appears to be properly configured as a supplicant, but cannot gain access to the intended authenticator port on the switch to which it is connected.** If **aaa authentication port-access** is configured for Local, ensure that you have entered the local *login* (operator-level) username and password of the authenticator switch into the **identity** and **secret** parameters of the supplicant configuration. If instead, you enter the enable (manager-level) username and password, access will be denied.

**The supplicant statistics listing shows multiple ports with the same authenticator MAC address.** The link to the authenticator may have been moved from one port to another without the supplicant statistics having been cleared from the first port. Refer to "Note on Supplicant Statistics" in the chapter on Port-Based and User-Based Access Control in the *Access Security Guide* for your switch.

**The show port-access authenticator < *port-list* > command shows one or more ports remain open after they have been configured with control unauthorized.** 802.1X is not active on the switch. After you execute **aaa port-access authenticator active**, all ports configured with **control unauthorized** should be listed as **Closed**.

```
HP Switch(config)# show port-access authenticator e 9
 Port Access Authenticator Status
  Port-access authenticator activated [No] : No
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

             Access   Authenticator  Authenticator
  Port Status Control  State          Backend State
  ---- ------ -------- -------------- --------------
  9    Open   FU       Force Auth     Idle

HP Switch(config)# show port-access authenticator active

HP Switch(config)# show port-access authenticator e 9
 Port Access Authenticator Status
  Port-access authenticator activated [No] : No
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

             Access   Authenticator  Authenticator
  Port Status Control  State          Backend State
  ---- ------ -------- -------------- --------------
  9    Closed FU       Force Unauth     Idle
```

Port 9 shows an "Open" status even though Access Control is set to **Unauthorized** (Force Auth). This is because the port-access authenticator has not yet been activated.

**Figure C-1. Authenticator Ports Remain "Open" Until Activated**

**RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch.** Use **show radius** to verify that the encryption key (RADIUS secret key) the switch is using is correct for the server being contacted. If the switch has only a global key configured, then it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, then it overrides the global key and must match the server key.

```
    10.33.13.119(config)# show radius
     Status and Counters - General RADIUS Information
      Deadtime(min) : 0
      Timeout(secs) : 5
      Retransmit Attempts : 3
      Global Encryption Key : My-Global-Key
      Dynamic Authorization UDP Port : 3799

                      Auth Acct DM/ Time
      Server IP Addr  Port Port CoA Window Encryption Key
      --------------- ---- ---- --- ------ ----------------
      10.33.18.119    1812 1813           119-only-key
```

Global RADIUS Encryption Key

Unique RADIUS Encryption Key for the RADIUS server at 10.33.18.119

**Figure C-2. Displaying Encryption Keys**

Also, ensure that the switch port used to access the RADIUS server is not blocked by an 802.1X configuration on that port. For example, **show port-access authenticator < *port-list* >** gives you the status for the specified ports. Also, ensure that other factors, such as port security or any 802.1X configuration on the RADIUS server are not blocking the link.

**The authorized MAC address on a port that is configured for both 802.1X and port security either changes or is re-acquired after execution of aaa port-access authenticator < *port-list* > initialize.** If the port is force-authorized with **aaa port-access authenticator <port-list> control authorized** command and port security is enabled on the port, then executing **initialize** causes the port to clear the learned address and learn a new address from the first packet it receives after you execute **initialize**.

**A trunked port configured for 802.1X is blocked.** If you are using RADIUS authentication and the RADIUS server specifies a VLAN for the port, the switch allows authentication, but blocks the port. To eliminate this problem, either remove the port from the trunk or reconfigure the RADIUS server to avoid specifying a VLAN.

## QoS-Related Problems

**Loss of communication when using VLAN-tagged traffic.** If you cannot communicate with a device in a tagged VLAN environment, ensure that the device either supports VLAN tagged traffic or is connected to a VLAN port that is configured as **Untagged**.

## Radius-Related Problems

**The switch does not receive a response to RADIUS authentication requests.** In this case, the switch will attempt authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

- Use **ping** to ensure that the switch has access to the configured RADIUS server.
- Verify that the switch is using the correct encryption key for the designated server.
- Verify that the switch has the correct IP address for the RADIUS server.

- Ensure that the **radius-server timeout** period is long enough for network conditions.
- Verify that the switch is using the same UDP port number as the server.

**RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch.** Use **show radius** to verify that the encryption key the switch is using is correct for the server being contacted. If the switch has only a global key configured, then it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, then it overrides the global key and must match the server key.

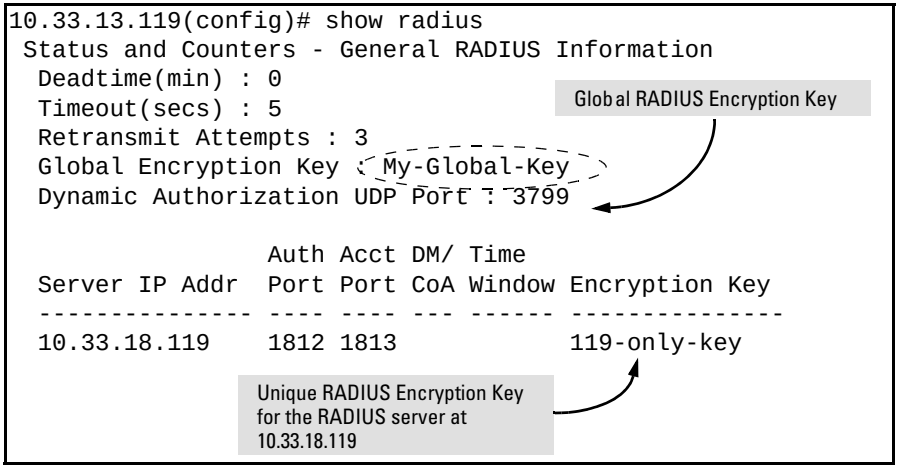



**Figure C-3. Examples of Global and Unique Encryption Keys**

## Spanning-Tree Protocol (MSTP) and Fast-Uplink Problems

**Caution**

If you enable MSTP, it is recommended that you leave the remainder of the MSTP parameter settings at their default values until you have had an opportunity to evaluate MSTP performance in your network. Because incorrect MSTP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how MSTP operates. To learn the details of MSTP operation, refer to the IEEE 802.1s standard.

**Broadcast Storms Appearing in the Network.** This can occur when there are physical loops (redundant links) in the topology.Where this exists, you should enable MSTP on all bridging devices in the topology in order for the loop to be detected.

**STP Blocks a Link in a VLAN Even Though There Are No Redundant Links in that VLAN.** In 802.1Q-compliant switches MSTP blocks redundant physical links even if they are in separate VLANs. A solution is to use only one, multiple-VLAN (tagged) link between the devices. Also, if ports are available, you can improve the bandwidth in this situation by using a port trunk. Refer to "Spanning Tree Operation with VLANs" in the chapter titled "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

**Fast-Uplink Troubleshooting.** Some of the problems that can result from incorrect usage of Fast-Uplink MSTP include temporary loops and generation of duplicate packets.

Problem sources can include:

- Fast-Uplink is configured on a switch that is the MSTP root device.
- Either the **Hello Time** or the **Max Age** setting (or both) is too long on one or more switches. Return the **Hello Time** and Max Age settings to their default values (2 seconds and 20 seconds, respectively, on a switch).
- A "downlink" port is connected to a switch that is further away (in hop count) from the root device than the switch port on which fast-uplink MSTP is configured.
- Two edge switches are directly linked to each other with a fast-uplink (Mode = **Uplink**) connection.
- Fast uplink is configured on both ends of a link.
- A switch serving as a backup MSTP root switch has ports configured for fast-uplink MSTP and has become the root device due to a failure in the original root device.

## SSH-Related Problems

**Switch access refused to a client.** Even though you have placed the client's public key in a text file and copied the file (using the **copy tftp pub-key-file** command) into the switch, the switch refuses to allow the client to have access. If the source SSH client is an SSHv2 application, the public key may be in the PEM format, which the switch (SSHv1) does not interpret. Check the SSH client application for a utility that can convert the PEM-formatted key into an ASCII-formatted key.

**Executing IP SSH does not enable SSH on the switch.** The switch does not have a host key. Verify by executing show ip host-public-key. If you see the message

```
ssh cannot be enabled until a host key is configured
(use 'crypto' command).
```

then you need to generate an SSH key pair for the switch. To do so, execute **crypto key generate**.(Refer to "2. Generating the Switch's Public and Private Key Pair" in the SSH chapter of the *Access Security Guide* for your switch.)

**Switch does not detect a client's public key that does appear in the switch's public key file (show ip client-public-key).** The client's public key entry in the public key file may be preceded by another entry that does not terminate with a new line (CR). In this case, the switch interprets the next sequential key entry as simply a comment attached to the preceding key entry. Where a public key file has more than one entry, ensure that all entries terminate with a new line (CR). While this is optional for the last entry in the file, not adding a new line to the last entry creates an error potential if you either add another key to the file at a later time or change the order of the keys in the file.

**An attempt to copy a client public-key file into the switch has failed and the switch lists one of the following messages.**

```
Download failed: overlength key in key file.

Download failed: too many keys in key file.

Download failed: one or more keys is not a valid RSA
public key.
```

The public key file you are trying to download has one of the following problems:

- A key in the file is too long. The maximum key length is 1024 characters, including spaces. This could also mean that two or more keys are merged together instead of being separated by a <CR><LF>.
- There are more than ten public keys in the key file.
- One or more keys in the file is corrupted or is not a valid rsa public key.

**Client ceases to respond ("hangs") during connection phase.** The switch does not support data compression in an SSH session. Clients will often have compression turned on by default, but will disable it during the negotiation phase. A client which does not recognize the compression-request

FAILURE response may fail when attempting to connect. Ensure that compression is turned off before attempting a connection to prevent this problem.

## TACACS-Related Problems

**Event Log.** When troubleshooting TACACS+ operation, check the switch's Event Log for indications of problem areas.

**All Users Are Locked Out of Access to the Switch.** If the switch is functioning properly, but no username/password pairs result in console or Telnet access to the switch, the problem may be due to how the TACACS+ server and/or the switch are configured. Use one of the following methods to recover:

- Access the TACACS+ server application and adjust or remove the configuration parameters controlling access to the switch.
- If the above method does not work, try eliminating configuration changes in the switch that have not been saved to flash (boot-up configuration) by causing the switch to reboot from the boot-up configuration (which includes only the configuration changes made prior to the last **write memory** command.) If you did not use **write memory** to save the authentication configuration to flash, then pressing the Reset button or cycling the power reboots the switch with the boot-up configuration.
- Disconnect the switch from network access to any TACACS+ servers and then log in to the switch using either Telnet or direct console port access. Because the switch cannot access a TACACS+ server, it will default to local authentication. You can then use the switch's local Operator or Manager username/password pair to log on.
- As a last resort, use the Clear/Reset button combination to reset the switch to its factory default boot-up configuration. Taking this step means you will have to reconfigure the switch to return it to operation in your network.

**No Communication Between the Switch and the TACACS+ Server Application.** If the switch can access the server device (that is, it can **ping** the server), then a configuration error may be the problem. Some possibilities include:

- The server IP address configured with the switch's tacacs-server host command may not be correct. (Use the switch's **show tacacs-server** command to list the TACACS+ server IP address.)

- The encryption key configured in the server does not match the encryption key configured in the switch (by using the **tacacs-server key** command). Verify the key in the server and compare it to the key configured in the switch. (Use **show tacacs-server** to list the global key. Use **show config** or **show config running** to list any server-specific keys.)
- The accessible TACACS+ servers are not configured to provide service to the switch.

**Access Is Denied Even Though the Username/Password Pair Is Correct.** Some reasons for denial include the following parameters controlled by your TACACS+ server application:

- The account has expired.
- The access attempt is through a port that is not allowed for the account.
- The time quota for the account has been exhausted.
- The time credit for the account has expired.
- The access attempt is outside of the time frame allowed for the account.
- The allowed number of concurrent logins for the account has been exceeded

For more help, refer to the documentation provided with your TACACS+ server application.

**Unknown Users Allowed to Login to the Switch.** Your TACACS+ application may be configured to allow access to unknown users by assigning them the privileges included in a *default user* profile. Refer to the documentation provided with your TACACS+ server application.

**System Allows Fewer Login Attempts than Specified in the Switch Configuration.** Your TACACS+ server application may be configured to allow fewer login attempts than you have configured in the switch with the **aaa authentication num-attempts** command.

## TimeP, SNTP, or Gateway Problems

**The Switch Cannot Find the Time Server or the Configured Gateway .**

TimeP, SNTP, and Gateway access are through the primary VLAN, which in the default configuration is the DEFAULT_VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

## VLAN-Related Problems

**None of the devices assigned to one or more VLANs on an 802.1Q-compliant switch are being recognized.** If multiple VLANs are being used on ports connecting 802.1Q-compliant devices, inconsistent VLAN IDs may have been assigned to one or more VLANs. For a given VLAN, the same VLAN ID must be used on all connected 802.1Q-compliant devices.

**Link Configured for Multiple VLANs Does Not Support Traffic for One or More VLANs.** One or more VLANs may not be properly configured as "Tagged" or "Untagged". A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured the same on both ports. For example, VLAN_1 and VLAN_2 use the same link between switch "X" and switch "Y".

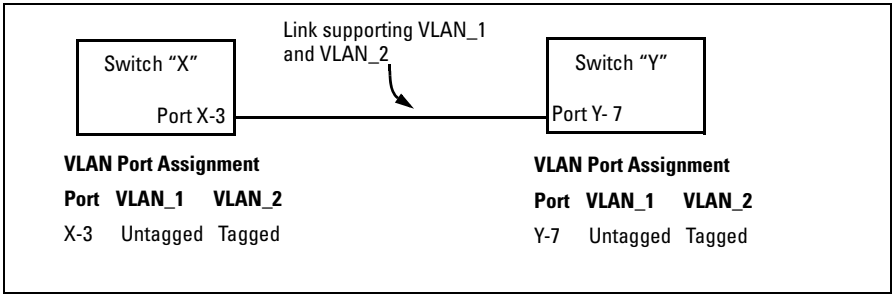



**Figure C-4. Example of Correct VLAN Port Assignments on a Link**

1. If VLAN_1 (VID=1) is configured as "Untagged" on port 3 on switch "X", then it must also be configured as "Untagged" on port 7 on switch "Y". Make sure that the VLAN ID (VID) is the same on both switches.
2. Similarly, if VLAN_2 (VID=2) is configured as "Tagged on the link port on switch "A", then it must also be configured as "Tagged" on the link port on switch "B". Make sure that the VLAN ID (VID) is the same on both switches.

**Duplicate MAC Addresses Across VLANs.** The switches covered in this guide operate with multiple forwarding databases. Thus, duplicate MAC addresses occurring on different VLANs can appear where a device having one MAC address is a member of more than one 802.1Q VLAN, and the switch port to which the device is linked is using VLANs (instead of MSTP or trunking) to establish redundant links to another switch. If the other device sends traffic over multiple VLANs, its MAC address will consistently appear in multiple VLANs on the switch port to which it is linked.

Note that attempting to create redundant paths through the use of VLANs will cause problems with some switches. One symptom is that a duplicate MAC address appears in the Port Address Table of one port, and then later appears on another port. While the switches have multiple forwarding databases, and thus does not have this problem, some switches with a single forwarding database for all VLANs may produce the impression that a connected device is moving among ports because packets with the same MAC address but different VLANs are received on different ports. You can avoid this problem by creating redundant paths using port trunks or spanning tree.

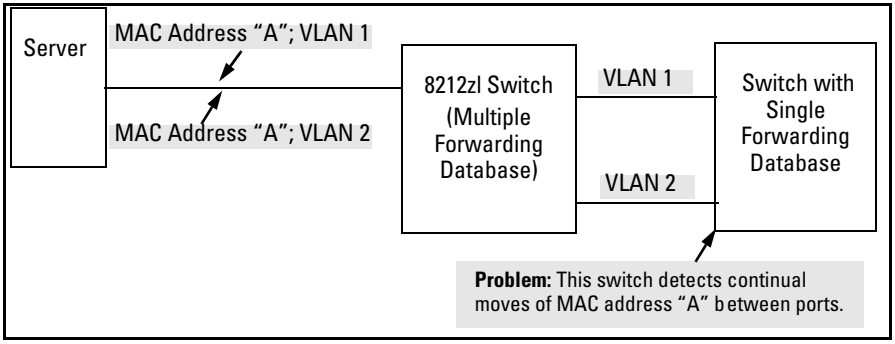



**Figure C-5. Example of Duplicate MAC Address**

## Fan Failure

When two or more fans fail, a two-minute timer starts. After two minutes, the switch is powered down and must be rebooted to restart it. This protects the switch from possible overheating.

HPrecommends that you replace a failed fan tray assembly within one minute of removing it.

# Using the Event Log for Troubleshooting Switch Problems

The Event Log records operating events in single- or double-line entries and serves as a tool to isolate and troubleshoot problems.

Entries are listed in chronological order, from the oldest to the most recent.

Once the log has received 2000 entries, it discards the oldest message each time a new message is received. The Event Log window contains 14 log entry lines. You can scroll through it to view any part of the log.

**Note**

The Event Log is *erased* if power to the switch is interrupted or if you enter the **boot system** command. The contents of the Event Log are *not* erased if you:

- Reboot the switch by choosing the **Reboot Switch** option from the menu interface.
- Enter the **reload** command from the CLI.

## Event Log Entries

As shown in Figure C-6, each Event Log entry is composed of five or six fields, depending on whether numbering is turned on or not:

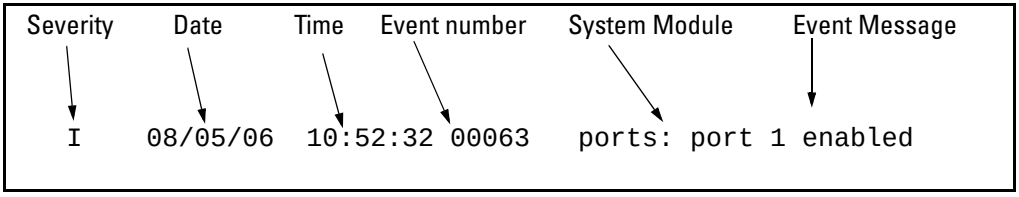



**Figure C-6.Format of an Event Log Entry**

***Severity*** is one of the following codes (from highest to lowest severity):

- **M** (major) indicates that a fatal switch error has occurred.
- **E** (error) indicates that an error condition occurred on the switch.
- **W** (warning) indicates that a switch service has behaved unexpectedly.
- **I** (information) provides information on normal switch operation.
- **D** (debug) is reserved for HPinternal diagnostic information.

***Date*** is the date in the format *mm/dd/yy* when an entry is recorded in the log.

***Time*** is the time in the format *hh:mm:ss* when an entry is recorded in the log.

***Event Number*** is the number assigned to an event. You can turn event numbering on and off with the [**no**] **log-number** command.

***System Module*** is the internal module (such as "ports:" for port manager) that generated a log entry. If VLANs are configured, then a VLAN name also appears for an event that is specific to an individual VLAN. Table C-1 lists the different system modules with a description of each one.

***Event Message*** is a brief description of the operating event.

**Table C-1. Event Log System Modules**

| System Module | Description | Documented in HPHardware/Software guide |
|---|---|---|
| 802.1x | 802.1X authentication: Provides access control on a per-client or per-port basis:<br>• Client-level security that allows LAN access to 802.1X clients (up to 32 per port) with valid user credentials<br>• Port-level security that allows LAN access only on ports on which a single 802.1X-capable client (supplicant) has entered valid RADIUS user credentials | *Access Security Guide* |
| addrmgr | Address Table Manager: Manages MAC addresses that the switch has learned and are stored in the switch's address table. | *Management and Configuration Guide* |
| auth | Authorization: A connected client must receive authorization through web, AMC, RADIUS-based, TACACS+-based, or 802.1X authentication before it can send traffic to the switch. | *Access Security Guide* |
| cdp | Cisco Discovery Protocol: Supports reading CDP packets received from neighbor devices, enabling a switch to learn about adjacent CDP devices. HP switches do not support the transmission of CDP packets to neighbor devices. | *Management and Configuration Guide* |
| console | Console interface used to monitor switch and port status, reconfigure the switch, read the event log through an in-band Telnet or out-of-band connection. | *Installation and Getting Started Guide* |
| cos | Class of Service (CoS): Provides priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet.<br>CoS messages also include Quality of Service (QoS) events. The QoS feature classifies and prioritizes traffic throughout a network, establishing an end-to-end traffic priority policy to manage available bandwidth and improve throughput of important data. | *Advanced Traffic Management Guide* |
| dhcp | Dynamic Host Configuration Protocol (DHCP) server configuration: Switch is automatically configured from a DHCP (Bootp) server, including IP address, subnet mask, default gateway, Timep Server address, and TFTP server address. | *Management and Configuration Guide* |

| System Module | Description | Documented in HPHardware/Software guide |
|---|---|---|
| dhcp v6c | DHCP for IPv6 prefix assignment | *IPv6 Management Guide* |
| dhcpr | DHCP relay: Forwards client-originated DHCP packets to a DHCP network server. | *Advanced Traffic Management Guide* |
| download | Download operation for copying a software version or files to the switch. | *Management and Configuration Guide* |
| dma | Direct Access Memory (DMA): Transmits and receives packets between the CPU and the switch. | — |
| fault | Fault Detection facility, including response policy and the sensitivity level at which a network problem should generate an alert. | *Management and Configuration Guide* |
| ffi | Find, Fix, and Inform: Event or alert log messages indicating a possible topology loop that cause excessive network activity and results in the network running slow. FFI messages include events on transceiver connections with other network devices. | *Installation and Getting Started Guide*<br>*Management and Configuration Guide* |
| garp | Generic Attribute Registration Protocol (GARP), defined in the IEEE 802.1D-1998 standard. | *Advanced Traffic Management Guide* |
| gvrp | GARP VLAN Registration Protocol (GVRP): Manages dynamic 802.1Q VLAN operations, in which the switch creates temporary VLAN membership on a port to provide a link to another port in the same VLAN on another device. | *Advanced Traffic Management Guide* |
| hpesp | Management module that maintains communication between switch ports. | *Installation and Getting Started Guide* |
| igmp | Internet Group Management Protocol: Reduces unnecessary bandwidth usage for multicast traffic transmitted from multimedia applications on a per-port basis. | *Advanced Traffic Management Guide* |
| ip | IP addressing: Configures the switch with an IP address and subnet mask to communicate on the network and support remote management access; configures multiple IP addresses on a VLAN. | *Management and Configuration Guide* |
| iplock | IP Lockdown: Prevents IP source address spoofing on a per-port and per-VLAN basis by forwarding only the IP packets in VLAN traffic that contain a known source IP address and MAC address binding for the port. | *Access Security Guide* |
| ipx | Novell Netware protocol filtering: On the basis of protocol type, the switch can forward or drop traffic to a specific set of destination ports on the switch. | *Access Security Guide* |
| lacp | LACP trunks: The switch can either automatically establish an 802.3ad-compliant trunk group or provide a manually configured, static LACP trunk. | *Management and Configuration Guide* |

| System Module | Description | Documented in HPHardware/Software guide |
|---|---|---|
| ldbal | Load balancing in LACP port trunks or 802.1s Multiple Spanning Tree protocol (MSTP) that uses VLANs in a network to improve network resource utilization and maintain a loop-free environment. | *Management and Configuration Guide*<br>*Advanced Traffic Management Guide* |
| lldp | Link-Layer Discovery Protocol: Supports transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices, enabling a switch to advertise itself to adjacent devices and to learn about adjacent LLDP devices. | *Management and Configuration Guide* |
| macauth | Web and MAC authentication: Port-based security employed on the network edge to protect private networks and the switch itself from unauthorized access using one of the following interfaces:<br>• Web page login to authenticate users for access to the network<br>• RADIUS server that uses a device's MAC address for authentication | *Access Security Guide* |
| maclock | MAC lockdown and MAC lockout<br>• MAC lockdown prevents station movement and MAC address "hijacking" by requiring a MAC address to be used only an assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN.<br>• MAC lockout blocks a specific MAC address so that the switch drops all traffic to or from the specified address. | *Access Security Guide* |
| mgr | IMC: Windows-based network management solutions for managing and monitoring performance of HPdevices. IMC messages also include events for configuration operations. | *Management and Configuration Guide* |
| netinet | Network Internet: Monitors the creation of a route or an Address Resolution Protocol (ARP) entry and sends a log message in case of failure. | *Advanced Traffic Management Guide* |
| pagp | Ports Aggregation Protocol (PAgP): Obsolete. Replaced by LACP (802.3ad). | — |
| ports | Port status and port configuration features, including mode (speed and duplex), flow control, and security settings.<br>Port messages include events on Power Over Ethernet (POE) operation and transceiver connections with other network devices. | *Installation and Getting Started Guide*<br>*Management and Configuration Guide*<br>*Access Security Guide* |
| radius | RADIUS (Remote Authentication Dial-In User Service) authentication and accounting: A network server is used to authenticate user-connection requests on the switch and collect accounting information to track network resource usage. | *Access Security Guide* |

| System Module | Description | Documented in HPHardware/Software guide |
|---|---|---|
| snmp | Simple Network Management Protocol: Allows you to manage the switch from a network management station, including support for security features, event reporting, flow sampling, and standard MIBs. | *Management and Configuration Guide* |
| sntp | Simple Network Time Protocol: Synchronizes and ensures a uniform time among interoperating devices. | *Management and Configuration Guide* |
| ssh | Secure Shell version 2 (SSHv2): Provides remote access to management functions on a switch via encrypted paths between the switch and management station clients capable of SSH operation.<br>SSH messages also include events from the Secure File Transfer Protocol (SFTP) feature. SFTP provides a secure alternative to TFTP for transferring sensitive information, such as switch configuration files, to and from the switch in an SSH session. | *Access Security Guide* |
| ssl | Secure Socket Layer Version 3 (SSLv3), including Transport Layer Security (TLSv1) support: Provides remote web access to a switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation. | *Access Security Guide* |
| stack | Stack management: Uses a single IP address and standard network cabling to manage a group (up to 16) of switches in the same IP subnet (broadcast domain), resulting in a reduced number of IP addresses and simplified management of small workgroups for scaling your network to handle increased bandwidth demand. | *Advanced Traffic Management Guide* |
| stp | Multiple-instance spanning tree protocol/MSTP (802.1s): Ensures that only one active path exists between any two nodes in a group of VLANs in the network. MSTP operation is designed to avoid loops and broadcast storms of duplicate messages that can bring down the network. | *Advanced Traffic Management Guide* |
| system | Switch management, including system configuration, switch bootup, activation of boot ROM image, memory buffers, traffic and security filters.<br>System messages also include events from Management interfaces (menu, CLI, web browser, IMC) used to reconfigure the switch and monitor switch status and performance. | *Management and Configuration Guide*<br>*Access Security Guide* |
| tacacs | TACACS+ authentication: A central server is used to control access to the switches (and other TACACS-aware devices) in the network through a switch's console port (local access) or Telnet (remote access). | *Access Security Guide* |
| tcp | Transmission Control Protocol: A transport protocol that runs on IP and is used to set up connections. | *Advanced Traffic Management Guide* |
| telnet | Session established on the switch from a remote device through the Telnet virtual terminal protocol. | *Management and Configuration Guide* |

| System Module | Description | Documented in HPHardware/Software guide |
|---|---|---|
| tftp | Trivial File Transfer Protocol: Supports the download of files to the switch from a TFTP network server. | *Management and Configuration Guide* |
| timep | Time Protocol: Synchronizes and ensures a uniform time among interoperating devices. | *Management and Configuration Guide* |
| update | Updates (TFTP or serial) to HPsoftware and updates to running-config and start-up config files | *Management and Configuration Guide* |
| vlan | Static 802.1Q VLAN operations, including port-and protocol-based configurations that group users by logical function instead of physical location<br>A port -based VLAN creates a layer-2 broadcast domain comprised of member ports that bridge IPv4 traffic among themselves.<br>VLAN messages include events from Management interfaces (menu, CLI, web browser, IMC) used to reconfigure the switch and monitor switch status and performance. | *Advanced Traffic Management Guide* |
| xmodem | Xmodem: Binary transfer feature that supports the download of software files from a PC or Unix workstation. | *Management and Configuration Guide* |

## Menu: Displaying and Navigating in the Event Log

To display the Event Log from the Main Menu, select **Event Log**. Figure C-7 shows a sample event log display.

```
Switch                                          25-Oct-2007  18:02:52
=========================-CONSOLE - MANAGER MODE -============================
M 10/25/07 16:30:02 sys: 'Operator cold reboot from CONSOLE session.'
I 10/25/07 17:42:51 00061 system: ------------------------------------------
I 10/25/07 17:42:51 00063 system: System went down:  10/25/07 16:30:02
I 10/25/07 17:42:51 00064 system: Operator cold reboot from CONSOLE session.
I 10/25/07 17:42:51 00433 ssh: Ssh server enabled
I 10/25/07 17:42:52 00400 stack: Stack Protocol disabled
I 10/25/07 17:42:52 00128 tftp: Enable succeeded
I 10/25/07 17:42:52 00417 cdp: CDP enabled

----  Log events stored in memory 1-751.  Log events on screen 690-704.

 Actions->   Back     Next page     Prev page     End     Help

Return to previous screen.
Use up/down arrow to scroll one line, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure C-7. Example of an Event Log Display**

The *log status line* below the recorded entries states the total number of events stored in the event log and which logged events are currently displayed.

To scroll to other entries in the Event Log, either preceding or following the currently visible portion, press the keys indicated at the bottom of the display (**Back, Next page**, **Prev page**, or **End**) or the keys described in Tabletable C-1.

**Table C-1. Event Log Control Keys**

| Key | Action |
|---|---|
| **[N]** | Advances the display by one page (next page). |
| **[P]** | Rolls back the display by one page (previous page). |
| **[v]** | Advances display by one event (down one line). |
| **[^]** | Rolls back display by one event (up one line). |
| **[E]** | Advances to the end of the log. |
| **[H]** | Displays Help for the Event Log. |

## CLI: Displaying the Event Log

To display messages recorded in the event log from the CLI, enter the **show logging** command. Keyword searches are supported.

***Syntax:*** show logging [-a, -r] [<*search-text*>]

*By default, the* **show logging** *command displays the log messages recorded since the last reboot in chronological order.*
**-a** *displays all recorded log messages, including those before the last reboot.*
**-r** *displays all recorded log messages, with the most recent entries listed first.*
<*search-text*> *displays all Event Log entries that contain the specified text. Use a* <*search-text*> *value with* **-a** *or* **-r** *to further filter* **show logging** *command output.*

**Examples.** To display all Event Log messages that have “system” in the message text, enter the following command:

```
HP Switch# show logging -a system
```

To display all Event Log messages recorded since the last reboot that have the word, “system”, in the message text, enter:

```
HP Switch# show logging system
```

## CLI: Clearing Event Log Entries

Use the **clear logging** command to hide, but not erase, Event Log entries displayed in **show logging** command output. Only new entries generated after you enter the command will be displayed.

To redisplay all hidden entries, including Event Log entries recorded prior to the last reboot, enter the **show logging -a** command.

***Syntax:*** clear logging

*Removes all entries from the event log display output.*

## CLI: Turning Event Numbering On or Off

***Syntax:*** [no] log-numbers

*Turns event numbering on and off*

## Using Log Throttling to Reduce Duplicate Event Log and SNMP Messages

A recurring event can generate a series of duplicate Event Log messages and SNMP traps in a relatively short time. As a result, the Event Log and any configured SNMP trap receivers may be flooded with excessive, exactly identical messages. To help reduce this problem, the switch uses *log throttle periods* to regulate (throttle) duplicate messages for recurring events, and maintains a counter to record how many times it detects duplicates of a particular event since the last system reboot.

When the first instance of a particular event or condition generates a message, the switch initiates a log throttle period that applies to all recurrences of that event. If the logged event recurs during the log throttle period, the switch increments the counter initiated by the first instance of the event, but does not generate a new message.

If the logged event repeats again after the log throttle period expires, the switch generates a duplicate of the first message, increments the counter, and starts a new log throttle period during which any additional instances of the event are counted, but not logged. Thus, for a particular recurring event, the switch displays only one message in the Event Log for each log throttle period in which the event reoccurs. Also, each logged instance of the event message includes counter data showing how many times the event has occurred since the last reboot. The switch manages messages to SNMP trap receivers in the same way.

## Log Throttle Periods

The length of the log throttle period differs according to an event's severity level:

| Severity Level | Log Throttle Period |
|---|---|
| I (Information) | 6000 Seconds |
| W (Warning) | 600 Seconds |
| D (Debug) | 60 Seconds |
| M (Major) | 6 Seconds |

## Example of Event Counter Operation

Suppose the switch detects the following after a reboot:

- Three duplicate instances of a "Send error" during the first log throttle period for this event
- Five more instances of the same Send error during the second log throttle period for this event
- Four instances of the same Send error during the third log throttle period for this event

In this case, the duplicate message would appear three times in the Event Log (once for each log throttle period for the event being described), and the Duplicate Message Counter would increment as shown in table C-2. (The same operation would apply for messages sent to any configured SNMP trap receivers.)

**Table C-2. How the Duplicate Message Counter Increments**

| Instances During 1st Log Throttle Period | Instances During 2nd Log Throttle Period | Instances During 3rd Log Throttle Period | Duplicate Message Counter* |
|---|---|---|---|
| 3 | | | 1 |
| | 5 | | 4 |
| | | 4 | 9 |

*This value always comprises the first instance of the duplicate message in the current log throttle period plus all previous occurrences of the duplicate message occurring since the switch last rebooted.

# Debug/Syslog Operation

While the Event Log records switch-level progress, status, and warning messages on the switch, the Debug/System Logging (*Syslog*) feature provides a way to record Event Log and debug messages on a remote device. For example, you can send messages about misconfigurations and other network protocol details to an external device, and later use them to debug network-level problems.

## Debug/Syslog Messaging

The Debug/Syslog feature allows you to specify the types of Event Log and debug messages that you want to send to an external device. As shown in Figure C-8, you can perform the following operations:

- Use the **debug** command to configure messaging reports for the following event types:
  - Events recorded in the switch's Event Log
  - LLDP events
  - SSH events
- Use the **logging** command to select a subset of Event Log messages to send to an external device for debugging purposes according to:
  - Severity level
  - System module

## Debug/Syslog Destination Devices

To use Debug/Syslog messaging, you must configure an external device as the logging destination by using the **logging** and **debug destination** commands. For more information, see "Debug Destinations" on page C-35 and "Configuring a Syslog Server" on page C-37.

A Debug/Syslog destination device can be a Syslog server and/or a console session. You can configure debug and logging messages to be sent to:

- Up to six Syslog servers
- A CLI session through a direct RS-232 console connection, or a Telnet or SSH session

## Debug/Syslog Configuration Commands

| | | |
|---|---|---|
| Event Notification Logging | — | Automatically sends switch-level event messages to the switch's Event Log. Debug and Syslog do not affect this operation, but add the capability of directing Event Log messaging to an external device. |
| **logging** Command | ***<syslog-ip-addr>*** | Enables Syslog messaging to be sent to the specified IP address. |
| | **facility** | (Optional) The **logging facility** command specifies the destination (facility) subsystem used on a Syslog server for debug reports. |
| | **priority-desc** | A text string associated with the values of facility, severity, and system-module. |
| | **severity** | Sends Event Log messages of equal or greater severity than the specified value to configured debug destinations. (The default setting is to send Event Log messages from all severity levels.) |
| | **system-module** | Sends Event Log messages from the specified system module to configured debug destinations. The severity filter is also applied to the system-module messages you select.<br>The default setting is to send Event Log messages from all system modules. To restore the default setting, enter the **no logging system-module** <*system-module*> or **logging system-module all-pass** commands. |
| **debug** Command | **all** | Sends debug logging to configured debug destinations for all Event Log options. |

| | |
|---|---|
| **destination** | **logging:** Disables or re-enables Syslog logging on one or more Syslog servers configured with the logging < *syslog-ip-addr* > command. See "Debug Destinations" on page C-35.<br>**session:** Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output. "Debug Destinations" on page C-35.<br>**buffer:** Enables Syslog logging to send the debug message types specified by the debug < debug-type > command to a buffer in switch memory. See "Debug Destinations" on page C-35.<br>**windshell:** print debug messages to windshell. |
| **event** | Sends standard Event Log messages to configured debug destinations. (The same messages are also sent to the switch's Event Log, regardless of whether you enable this option.) |
| **ip** | **forwarding:** Sends IPv4 forwarding messages to the debug destination(s).<br>**packet:** Sends IPv4 packet messages to the debug destination(s).<br>**rip:** Sends RIP event logging to the debug destination(s). |
| **ipv6** | **dhcpv6-client:** Sends DHCPv6 client debug messages to the configured debug destination.<br>**forwarding:** Sends IPv6 forwarding messages to the debug destination(s)<br>**nd:** Sends IPv6 debug messages for IPv6 neighbor discovery to the configured debug destination(s).<br>**packet:** Sends IPv6 packet messages to the debug destination(s). |
| **lldp** | Sends LLDP debug logging to the debug destination(s). |
| **ssh** | Sends SSH debug messages at the specified level to the debug destination. The levels are fatal, error, info, verbose, debug, debug2, and debug3. |

**Figure C-8. Summary of Debug/Syslog Configuration Commands**

Using the Debug/Syslog feature, you can perform the following operations:

- Configure the switch to send Event Log messages to one or more Syslog servers. In addition, you can configure the messages to be sent to the User log facility (default) or to another log facility on configured Syslog servers.

**Note**

As of November 2008, the **logging facility** < *facility-name* > option (described on page C-39) is supported on the following switch models:

- 8212zl switch
- Series 6400cl switches
- 6200yl Switch
- Series 5400zl switches
- Series 5300xl switches
- Series 4200vl switches
- Series 4100gl switches (software release G.07.50 or greater)

- Series 3500yl switches
- Series 3400cl switches
- Series 2910al switches
- Series 2900 switches
- Series 2800 switches
- Series 2610 switches
- Series 2600 switches and the Switch 6108 (software release H.07.30 or greater)
- Series 2520 switches

For the latest feature information on HP switches, visit the HPNetworking web site and check the latest release notes for the switch products you use.

- Configure the switch to send Event Log messages to the current management-access session (serial-connect CLI, Telnet CLI, or SSH).
- Disable all Syslog debug logging while retaining the Syslog addresses from the switch configuration. This allows you to configure Syslog messaging and then disable and re-enable it as needed.
- Display the current debug configuration. If Syslog logging is currently active, the list f configured Syslog servers is displayed.
- Display the current Syslog server list when Syslog logging is disabled.

## Configuring Debug/Syslog Operation

1. To use a Syslog server as the destination device for debug messaging, follow these steps:
   a. Enter the **logging** < *syslog-ip-addr* > command at the global configuration level to configure the Syslog server IP address and enable Syslog logging. Optionally, you may also specify the destination subsystem to be used on the Syslog server by entering the **logging facility** command.

      If no other Syslog server IP addresses are configured, entering the **logging** command enables both debug messaging to a Syslog server and the Event debug message type. As a result, the switch automatically sends Event Log messages to the Syslog server, regardless of other debug types that may be configured.

   b. Re-enter the **logging** command in Step “a” to configure additional Syslog servers. You can configure up to a total of six servers. (When multiple server IP addresses are configured, the switch sends the debug message types that you configure in Step 3 to all IP addresses.)

2. To use a CLI session on a destination device for debug messaging:
   a. Set up a serial, Telnet, or SSH connection to access the switch's CLI.
   b. Enter the **debug destination session** command at the manager level.
3. Enable the types of debug messages to be sent to configured Syslog servers and/or the current session device by entering the **debug** < *debug-type* > command:

   ```
   HP Switch# debug <all|destination|event|ip|ipv6
   |lldp|ssh>
   ```

   Repeat this step if necessary to enable multiple debug message types.

   By default, Event Log messages are sent to configured debug destination devices. To block Event Log messages from being sent, enter the **no debug event** command.
4. If necessary, enable a subset of Event Log messages to be sent to configured Syslog servers by specifying a severity level and/or system module using the following commands

```
HP Switch(config)# logging severity <debug | major | error | warning | info >
HP Switch(config)# logging system-module < system-module >
```

   To display a list of valid values for each command, enter **logging severity** or **logging system-module** followed by **?** or pressing the **Tab** key.

   The severity levels in order from the highest to lowest severity are: major, error, warning, info, debug. For a list of valid values for the **logging system-module** <*system-module* > command, refer to Table C-1 on page C-18.
5. If you configure system-module and/or severity-level values to filter Event Log messages, when you finish troubleshooting, you may want to reset these values to their default settings so that the switch sends all Event Log messages to configured debug destinations (Syslog servers and/or CLI session).

   To remove a configured setting and restore the default values that send all Event Log messages, enter one or both of the following commands:

```
HP Switch(config)# no logging severity <debug | major | error | warning | info>
HP Switch(config)# no logging system-module < system-module >
```

**Caution**

If you configure a severity-level, system-module, logging destination, or logging facility value and save the settings to the startup configuration (for example, by entering the **write memory** command), the debug settings are saved after a system reboot (power cycle or reboot) and re-activated on the switch. As a result, after switch startup, one of the following situations may occur:

- Only a partial set of Event Log messages may be sent to configured debug destinations.
- Messages may be sent to a previously configured Syslog server used in an earlier debugging session.

## Displaying a Debug/Syslog Configuration

Use the **show debug** command to display the currently configured settings for:

- Debug message types and Event Log message filters (severity level and system module) sent to debug destinations
- Debug destinations (Syslog servers or CLI session) and Syslog server facility to be used

***Syntax:*** show debug

*Displays the currently configured debug logging destinations and message types selected for debugging purposes. (If no Syslog server address is configured with the* **logging** *<syslog-ip-addr> command, no* **show debug** *command output is displayed.)*

```
HP Switch(config)# show debug

  Debug Logging
   Destination:
    Logging --
     10.28.38.164
     Facility=kern
     Severity=warning
     System module=all-pass
    Enabled debug types:
     event
```

**Figure C-9. Sample Output of show debug Command**

**Example:** In the following example, no Syslog servers are configured on the switch (default setting). When you configure a Syslog server, debug logging is enabled to send Event Log messages to the server. To limit the Event Log messages sent to the Syslog server, specify a set of messages by entering the **logging severity** and **logging system-module** commands.

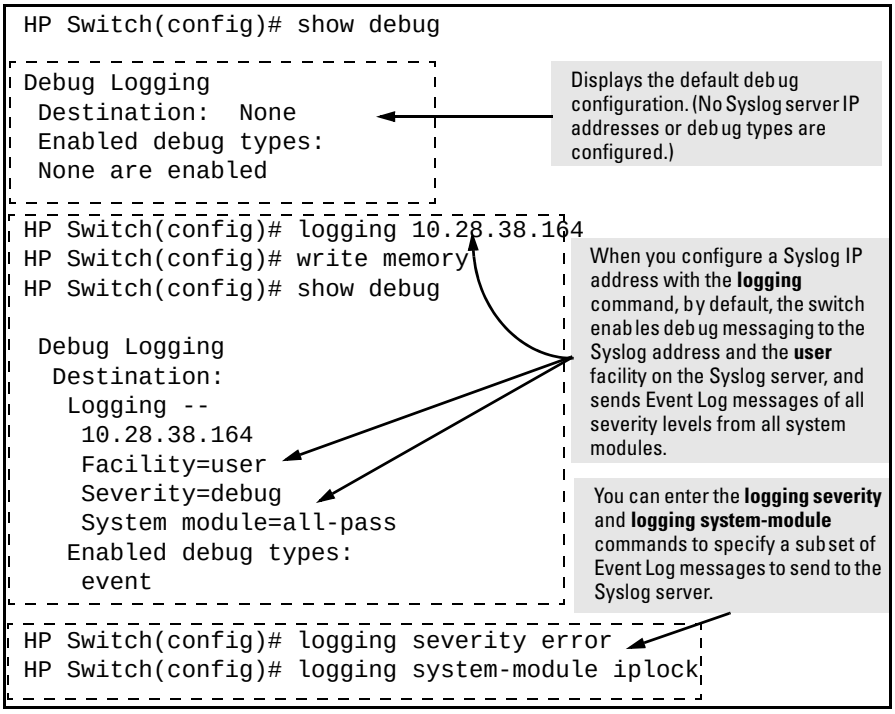



**Figure C-10. Syslog Configuration to Receive Event Log Messages From Specified System Module and Severity Levels**

As shown at the top of Figure C-10, if you enter the **show debug** command when no Syslog server IP address is configured, the configuration settings for Syslog server facility, Event Log severity level and system module are not displayed.

However, after you configure a Syslog server address and enable Syslog logging, all debug and logging settings are displayed with the **show debug** command. If you do not want Event Log messages sent to Syslog servers, you can block the messages from being sent by entering the **no debug event** command. (There is no effect on the normal logging of messages in the switch's Event Log.)

## Debug Command

At the manager level, use the **debug** command to perform two main functions:

- Specifies the types of event messages to be sent to an external destination.
- Specifies the destinations to which selected message types are sent.

By default, no debug destination is enabled and only Event Log messages are enabled to be sent.

**Note**

To configure a Syslog server, use the **logging** <*syslog-ip-addr*> command. For more information, see "Configuring a Syslog Server" on page C-37.

## Debug Messages

Use the **debug** command to configure the types of debug messages that the switch can send to configured debug destinations.

***Syntax:*** [no] debug < *debug-type* >

all

*Configures the switch to send all debug message types to configured debug destination(s). (Default: Disabled - No debug messages are sent.)*

cdp

*Sends CDP information to configured debug destinations.*

destination

**logging**—*Disables or re-enables Syslog logging on one or more Syslog servers configured with the* **logging** < *syslog-ip-addr* > *command. See "Debug Destinations" on page C-35.*
**session**—*Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output. "Debug Destinations" on page C-35.*
**buffer**—*Enables Syslog logging to send the debug message types specified by the* **debug** < *debug-type* > *command to a buffer in switch memory. See "Debug Destinations" on page C-35.*

event

*Configures the switch to send Event Log messages to configured debug destinations.*
***Note:*** *This value does not affect the reception of event notification messages in the Event Log on the switch.*

*Event Log messages are automatically enabled to be sent to debug destinations in these conditions:*

- *If no Syslog server address is configured and you enter the* **logging** *<syslog-ip-addr> command to configure a destination address.*
- *If at least one Syslog server address is configured in the startup configuration and the switch is rebooted or reset.*

*Event log messages are the default type of debug message sent to configured debug destinations.*

ip [fib | packet ]

*Sends IP messages to configured destinations.*

ip [fib [events]]

*For the configured debug destinations:*
**events***—Sends IP Forwarding Information Base events.*

ip [packet]

*Enables the specified PIM message type*

ipv6 [dhcpv6-client | nd | packet]

***Note****: See the "IPv6 Diagnostic and Troubleshooting" chapter in the IPv6 Configuration Guide for your switch for more detailed IPv6 debug options.*
*When no debug options are included, displays debug messages for all IPv6 debug options.*
**dhcpv6-client [events | packet]***—Displays DHCPv6 client event and packet data.*
**nd***—Displays debug messages for IPv6 neighbor discovery.*
**packet***—Displays IPv6 packet messages.*

lldp

*Enables all LLDP message types for the configured destinations.*

security [ port-access | port-security | radius-server | ssh | tacacs-server | user-profile-mib]

**port-access**—*Sends port-access debug messages to the debug destination.*
**radius-server—***Sends RADIUS debug messages to the debug destination.*
**ssh—***Sends SSH debug messages at the specified level to the debug destination. The levels are fatal, error, info, verbose, debug, debug2, and debug3.*
**tacacs-server—***Sends TACACS debug messages to the debug destination.*
**user-profile-mib—***Sends user profile MIB debug messages to the debug destination.*

snmp < pdu >

*Displays the SNMP debug messages.*
**pdu**—*Displays SNMP pdu debug messages.*

## Debug Destinations

Use the **debug destination** command to enable (and disable) Syslog messaging on a Syslog server or to a CLI session for specified types of debug and Event Log messages.

***Syntax:*** [no] debug destination < logging | session | buffer >

logging

*Enables Syslog logging to configured Syslog servers so that the debug message types specified by the* **debug** <*debug-type*> *command (see "Debug Messages" on page C-33) are sent. (Default: Logging disabled)*
*To configure a Syslog server IP address, refer to "Configuring a Syslog Server" on page C-37.*

***Note:*** *Debug messages from the switches covered in this guide have a debug severity level. Because the default configuration of some Syslog servers ignore Syslog messages with the debug severity level, ensure that the Syslog servers you want to use to receive debug messages are configured to accept the debug level. For more information, refer to "Operating Notes for Debug and Syslog" on page C-43.*

session

*Enables transmission of event notification messages to the CLI session that most recently executed this command. The session can be on any one terminal emulation device with serial, Telnet, or SSH access to the CLI at the Manager level prompt (***HP Switch#_** *). If more than one terminal device has a console session with the CLI, you can redirect the destination from the current device to another device. Do so by executing* **debug destination session** *in the CLI on the terminal device on which you now want to display event messages.*
*Event message types received on the selected CLI session are configured with the* **debug** < *debug-type* > *command. (Refer to* "Debug Messages" on page C-33*.)*

buffer

*Enables Syslog logging to send the debug message types specified by the* **debug** < *debug-type* > *command to a buffer in switch memory. To view the debug messages stored in the switch buffer, enter the* **show debug buffer** *command.*

## Logging Command

At the global configuration level, the **logging** command allows you to enable debug logging on specified Syslog servers and select a subset of Event Log messages to send for debugging purposes according to:

- Severity level
- System module

By specifying both a severity level and system module, you can use both configured settings to filter the Event Log messages you want to use to troubleshoot switch or network error conditions.

**Caution**

After you configure a Syslog server and a severity level and/or system module to filter the Event Log messages that are sent, if you save these settings to the startup configuration file by entering the **write memory** command, these debug and logging settings are automatically re-activated after a switch reboot or power recycle. The debug settings and destinations configured in your previous troubleshooting session will then be applied to the current session, which may not be desirable.

After a reboot, messages remain in the Event Log and are not deleted. However, after a power recycle, all Event Log messages are deleted.

If you configure a severity level and/or system module to temporarily filter Event Log messages, be sure to reset the values to their default settings by entering the **no** form of the following commands to ensure that Event Log messages of all severity levels and from all system modules are sent to configured Syslog servers:

```
HP Switch(config)# no logging severity <debug|major|error|warning|info>
HP Switch(config)# no logging system-module <system-module>
```

## Configuring a Syslog Server

Syslog is a client-server logging tool that allows a client switch to send event notification messages to a networked device operating with Syslog server software. Messages sent to a Syslog server can be stored to a file for later debugging analysis.

To use the Syslog feature, you must install and configure a Syslog server application on a networked host accessible to the switch. Refer to the documentation for the Syslog server application for instructions.

To configure a Syslog server, use the **logging** < *syslog-ip-addr* > command as described below.

When you configure a Syslog server, Event Log messages are automatically enabled to be sent to the server. To reconfigure this setting, use the following commands:

- Use **debug** command to specify additional debug message types (see "Debug Messages" on page C-33).
- Use the **logging** command to configure the system module or severity level used to filter the Event Log messages sent to configured Syslog servers (see "Configuring the Severity Level for Event Log Messages Sent to a Syslog Server" on page C-42 and "Configuring the System Module Used to Select the Event Log Messages Sent to a Syslog Server" on page C-42).

To display the currently configured Syslog servers as well as the types of debug messages and the severity-level and system-module filters used to specify the Event Log messages that are sent, enter the **show debug** command (see "Displaying a Debug/Syslog Configuration" on page C-31).

***Syntax:*** [no] logging < *syslog-ip-addr* >

*Enables or disables Syslog messaging to the specified IP address. You can configure up to six addresses. If you configure an address when none are already configured, this command enables destination logging (Syslog) and the Event debug type. Therefore, at a minimum, the switch begins sending Event Log messages to configured Syslog servers. (Refer to "Debug Messages" on page C-33.)*

**no logging** *removes all currently configured Syslog logging destinations from the running configuration.*

**no logging** < *syslog-ip-address* > *removes only the specified Syslog logging destination from the running configuration.*

*If you use the "***no***" form of the command to delete the only remaining Syslog server address, debug destination logging is disabled on the switch, but the default Event debug type is not changed.*

*Also, removing all configured Syslog destinations with the* **no logging** *command (or a specified Syslog server destination with the* **no logging** < *syslog-ip-address* > *command) does not delete the Syslog server IP addresses stored in the startup configuration. To delete Syslog addresses in the startup configuration, you must enter a* **no logging** *command followed by the* **write memory** *command. To verify the deletion of a Syslog server address, display the startup configuration by entering the* **show config** *command.*

*To block the messages sent to configured Syslog servers from the currently configured debug message type, enter the* **no debug** < *debug-type* > *command. (See "Debug Messages" on page C-33.)*

*To disable Syslog logging on the switch without deleting configured server addresses, enter the* **no debug destination logging** *command. Note that, unlike the case in which no Syslog servers are configured, if one or more Syslog servers are already configured and Syslog messaging is disabled, configuring a new server address does not re-enable Syslog messaging. To re-enable Syslog messaging, you must enter the* **debug destination logging** *command.*

***Syntax:*** [no] logging facility < *facility-name* >

*The logging facility specifies the destination subsystem used in a configured Syslog server. (All configured Syslog servers must use the same subsystem.) HPrecommends the default (user) subsystem unless your application specifically requires another subsystem. Options include:*

**user** *(default) — Random user-level messages*
**kern** *— Kernel messages*
**mail** *— Mail system*
**daemon** *— System daemons*
**auth** *— Security/Authorization messages*
**syslog** *— Messages generated internally by Syslog*
**lpr** *— Line-Printer subsystem*
**news** *— Netnews subsystem*
**uucp** *— uucp subsystem*
**cron** *— cron/at subsystem*
**sys9** *— cron/at subsystem*
**sys10 - sys14** *— Reserved for system use*
**local10 - local17** *— Reserved for system use*

*Use the* **no** *form of the command to remove the configured facility and reconfigure the default (***user***) value.*
*For a list of supported HP switches, refer to the page C-28 Note .*

## Adding a Description for a Syslog Server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP.

**Note**

The HP enterprise MIB hpicfSyslog.mib allows the configuration and monitoring of syslog for SNMP (RFC 3164 supported).

The CLI command is:

***Syntax:*** logging <ip-addr> control-descr <text_string>]
no logging <ip-addr> [control-descr]

*An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. IPv4 addresses only. Use the* **no** *form of the command to remove the description.*
*Limit: 255 characters*
***Note****: To remove the description using SNMP, set the description to an empty string.*

```
HP Switch(config)# logging 10.10.10.2 control-descr syslog_one
```

**Figure C-11. Example of the Logging Command with a Control Description**

**Caution**

Entering the **no logging** command removes ALL the syslog server addresses without a verification prompt.

## Adding a Priority Description

You can add a user-friendly description for the set of syslog filter parameters using the **priority-descr** option. The description can be added with the CLI or SNMP. The CLI command is:

***Syntax:*** logging priority-descr <text_string>
no logging priority-descr

*Provides a user-friendly description for the combined filter values of* **severity** *and* **system module**. *If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. Use the* **no** *form of the command to remove the description.*
*Limit: 255 characters*

```
HP Switch(config)# logging priority-descr severe-pri
```

**Figure C-12. Example of the Logging Command with a Priority Description**

**Note**

A notification is sent to the SNMP agent if there are any changes to the syslog parameters either through the CLI or with SNMP.

## Adding a Description for a Syslog Server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP.

**Note**

The HP enterprise MIB hpicfSyslog.mib allows the configuration and monitoring of syslog for SNMP (RFC 3164 supported).

The CLI command is:

***Syntax:*** logging <ip-addr> control-descr <text_string>]
no logging <ip-addr> [control-descr]

*An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. IPv4 addresses only. Use the* **no** *form of the command to remove the description.*
*Limit: 255 characters*
***Note****: To remove the description using SNMP, set the description to an empty string.*

```
HP Switch(config)# logging 10.10.10.2 control-descr syslog_one
```

**Figure C-13. Example of the Logging Command with a Control Description**

**Caution**

Entering the **no logging** command removes ALL the syslog server addresses without a verification prompt.

## Adding a Priority Description

You can add a user-friendly description for the set of syslog filter parameters using the **priority-descr** option. The description can be added with the CLI or SNMP. The CLI command is:

***Syntax:*** logging priority-descr <text_string>
no logging priority-descr

*Provides a user-friendly description for the combined filter values of* **severity** *and* **system module**. *If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. Use the* **no** *form of the command to remove the description.*
*Limit: 255 characters*

```
HP Switch(config)# logging priority-descr severe-pri
```

**Figure C-14. Example of the Logging Command with a Priority Description**

**Note**

A notification is sent to the SNMP agent if there are any changes to the syslog parameters either through the CLI or with SNMP.

## Configuring the Severity Level for Event Log Messages Sent to a Syslog Server

Event Log messages are entered with one of the following severity levels (from highest to lowest):

**Major:** A fatal error condition has occurred on the switch.

**Error:** An error condition has occurred on the switch.

**Warning:** A switch service has behaved unexpectedly.

**Information:** Information on a normal switch event.

**Debug:** Reserved for HPinternal diagnostic information.

Using the **logging severity** command, you can select a set of Event Log messages according to their severity level and send them to a Syslog server. Messages of the selected and higher severity will be sent. To configure a Syslog server, see "Configuring a Syslog Server" on page C-37.

***Syntax:*** [no] logging severity < major | error | warning | info | debug >

*Configures the switch to send all Event Log messages with a severity level equal to or higher than the specified value to all configured Syslog servers.*
*Default:* **debug** *(Reports messages of all severity levels.)*
*Use the* **no** *form of the command to remove the configured severity level and reconfigure the default value, which sends Event Log messages of all severity levels to Syslog servers.*
***Note:*** *The severity setting does not affect event notification messages that the switch normally sends to the Event Log. All messages remain recorded in the Event Log.*

## Configuring the System Module Used to Select the Event Log Messages Sent to a Syslog Server

Event Log messages contain the name of the system module that reported the event. Using the **logging system-module** command, you can select a set of Event Log messages according to the originating system module and send them to a Syslog server. To configure a Syslog server, see "Configuring a Syslog Server" on page C-37.

Using the **logging system-module** command, you can select messages from only one system module to be sent to a Syslog server. You cannot configure messages from multiple system modules to be sent. If you re-enter the command with a different system module name, the currently configured value is replaced with the new one.

***Syntax:*** [no] logging system-module < *system-module* >

*Configures the switch to send all Event Log messages being logged from the specified system module to configured Syslog servers.*
*Refer to Table C-1 on page C-27 for the correct value to enter for each system module.*
*Default:* **all-pass** *(Reports all Event Log messages.)*
*Use the* **no** *form of the command to remove the configured system module value and reconfigure the default value, which sends Event Log messages from all system modules to Syslog servers.*
***Note:*** *This setting has no effect on event notification messages that the switch normally sends to the Event Log.*

## Operating Notes for Debug and Syslog

- **Rebooting the Switch or pressing the Reset button resets the Debug Configuration.**

| Debug Option | Effect of a Reboot or Reset |
|---|---|
| logging (debug destination) | If Syslog server IP addresses are stored in the startup-config file, they are saved across a reboot and the logging destination option remains enabled. Otherwise, the logging destination is disabled. |
| session (debug destination) | Disabled. |
| All (debug type) | Disabled. |
| event (debug type) | If a Syslog server IP address is configured in the startup-config file, the sending of Event Log messages is reset to **enabled**, regardless of the last active setting.<br>If no Syslog server is configured, the sending of Event Log messages is **disabled**. |
| IP (debug type) | Disabled. |

- **Debug commands do not affect normal message output to the Event Log.**

  Using the **debug event** command, you can specify that Event Log messages are sent to the debug destinations you configure (CLI session and/or Syslog servers) in addition to the Event Log.

- **Ensure that your Syslog servers accept Debug messages.**

  All Syslog messages resulting from a debug operation have a "debug" severity level. If you configure the switch to send debug messages to a Syslog server, ensure that the server's Syslog application is configured to accept the "debug" severity level. (The default configuration for some Syslog applications ignores the "debug" severity level.)

- Duplicate IP addresses are not stored in the list of syslog servers.
- If the default severity value is in effect, all messages that have severities greater than the default value are passed to syslog. For example, if the default severity is "debug", all messages that have severities greater than debug are passed to syslog.
- There is a limit of six syslog servers. All syslog servers are sent the same messages using the same filter parameters. An error is generated for an attempt to add more than six syslog servers.

# Diagnostic Tools

### Diagnostic Features

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Port Auto negotiation | n/a | — | — | — |
| Ping test | n/a | — | page C-47 | page C-46 |
| Link test | n/a | — | page C-47 | page C-46 |
| Traceroute operation | n/a | — | page C-49 | n/a |
| View switch configuration files | n/a | — | page C-52 | page C-53 |
| View switch (show tech) operation | n/a | — | page C-53 | — |
| View crash information and command history | n/a | — | page C-55 | — |
| View system information and software version | n/a | — | page C-55 | — |
| Useful commands in a troubleshooting session | n/a | — | page C-59 | — |

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| Resetting factory-default configuration | page C-60 (Buttons) | — | page C-60 | — |
| Restoring a flash image | n/a | — | page C-61 | — |
| Port Status | n/a | page B-6 | page B-6 | page B-6 |

## Port Auto-Negotiation

When a link LED does not light (indicating loss of link between two devices), the most common reason is a failure of port auto-negotiation between the connecting ports. If a link LED fails to light when you connect the switch to a port on another device, do the following:

1. Ensure that the switch port and the port on the attached end-node are both set to **Auto** mode.
2. If the attached end-node does not have an **Auto** mode setting, then you must manually configure the switch port to the same setting as the end-node port. Refer to Chapter 2, “Port Status and Configuration”.

## Ping and Link Tests

The Ping test and the Link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

**Note**

To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

**Ping Test.** This is a test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests). To use the **ping** (or **traceroute**) command with host names or fully qualified domain names, refer to “DNS Resolver” on page C-63.

**Link Test.** This is a test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured). During the link test, IEEE 802.2 test packets are sent to the designated network device in the same VLAN or broadcast domain. The remote device must be able to respond with an 802.2 Test Response Packet.

## Web: Executing Ping or Link Tests

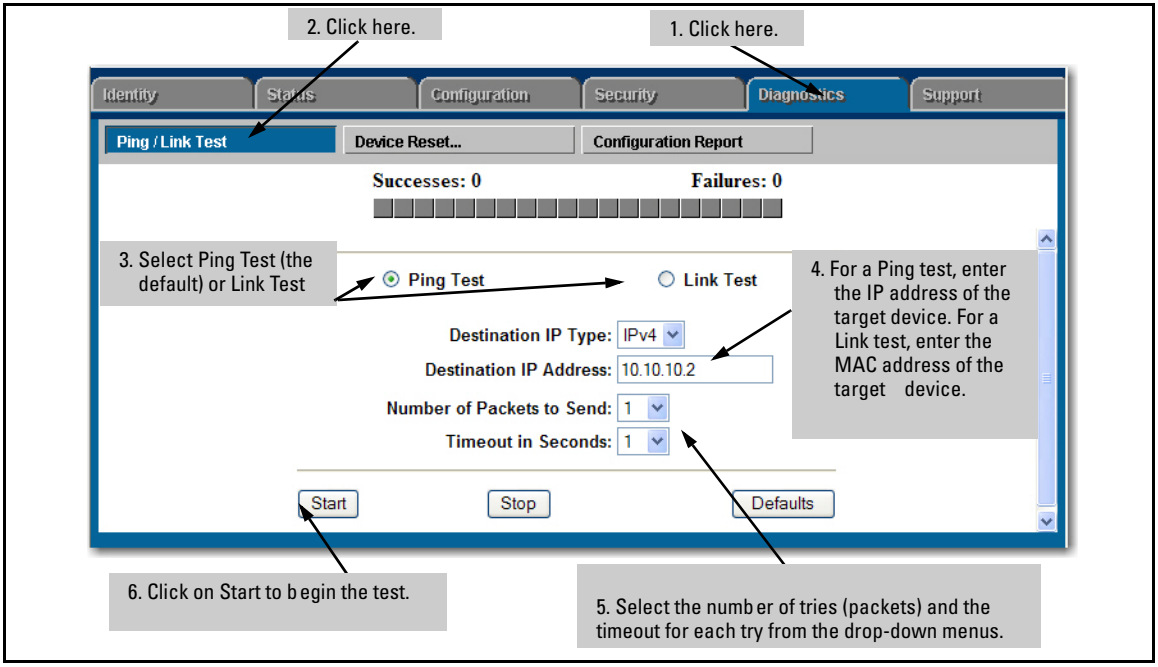



**Figure C-15. Link and Ping Test Screen on the Web Browser Interface**

**Successes** indicates the number of Ping or Link packets that successfully completed the most recent test.

**Failures** indicates the number of Ping or Link packets that were unsuccessful in the last test. Failures indicate connectivity or network performance problems (such as overloaded links or devices).

**Destination IP/MAC Address** is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the *X.X.X.X* format where *X* is a decimal number between 0 and 255. A MAC address is made up of 12 hexadecimal digits, for example, 0060b0-080400.

**Number of Packets to Send** is the number of times you want the switch to attempt to test a connection.

**Timeout in Seconds** is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

**To halt a Link or Ping test** before it concludes, click on the Stop button.
**To reset the screen** to its default settings, click on the Defaults button.

## CLI: Ping Test

The Ping (Packet InterNet Groper) test uses Internet Control Message Protocol (ICMP) echo requests and ICMP echo replies to determine if another device is alive. It also measures the amount of time it takes to receive a reply from the specified destination. The Ping command has several extended commands that allow advanced checking of destination availability.

***Syntax:*** ping <ip-address | hostname | switch-num> [repetitions <1-10000>] [timeout <1-60>] [source <ip-address> | <vlan-id>] [data-size <0 - 65471>] [data-fill <0-1024>]

ping6 <ip-address | hostname | switch-num> [repetitions <1-10000>] [timeout <1-60>] [source <ip-address> | <vlan-id>] [data-size <0 - 65471>] [data-fill <0-1024>]

*Sends ICMP echo requests to determine if another device is alive.*

***Note**: For information about* **ping6**, *see the "IPv6 Configuration Guide" for your switch.*

**<ip-address | hostname>**

*Target IP address or hostname of the destination node being pinged.*

**repetitions <1-10000>**

*Number of ping packets sent to the destination address. Default: 1*

**timeout <1-60>**

*Timeout interval in seconds; the ECHO REPLY must be received before this time interval expires for the Ping to be successful.*
*Default: 5*

**source <ip-addr | hostname >**

*Source IP address or hostname. The source IP address must be owned by the router. If a VLAN is specified, the IP address associated with the specified VLAN is used.*

**data-size <0-65471>**

*Size of packet sent. Default: 0 (zero)*

**data-fill <0-1024>**

*The data pattern in the packet. Default: Zero length string*

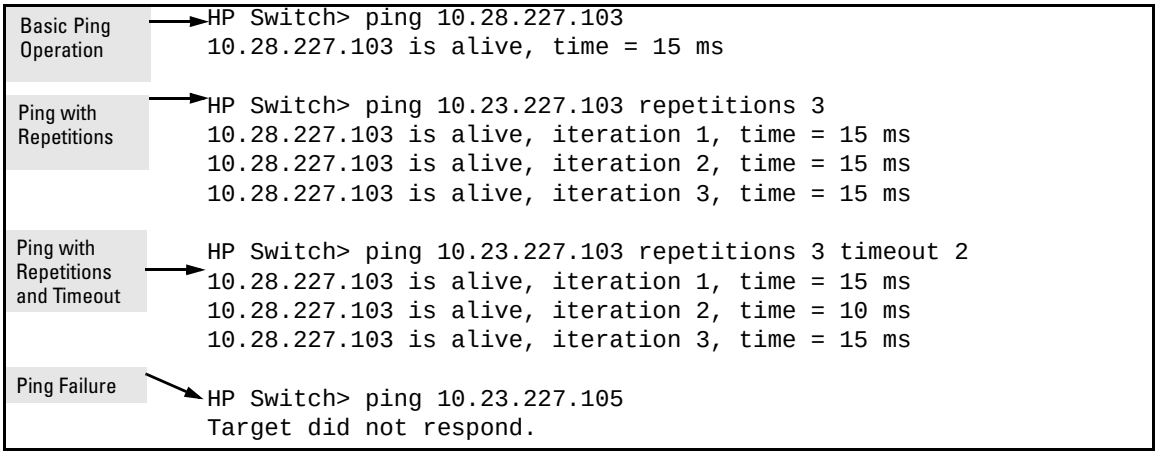



**Figure C-16. Examples of Ping Tests**

To halt a ping test before it concludes, press **[Ctrl] [C]**.

**Note**

To use the **ping** (or **traceroute**) command with host names or fully qualified domain names, refer to "DNS Resolver" on page C-63.

## Link Tests

You can issue single or multiple link tests with varying repetitions and timeout periods. The defaults are:

- Repetitions: 1 (1 - 999)
- Timeout: 5 seconds (1 - 256 seconds)

***Syntax:*** link < *mac-address* > [repetitions < 1 - 999 >] [timeout < 1 - 256 >] [vlan < *vlan-id* >]

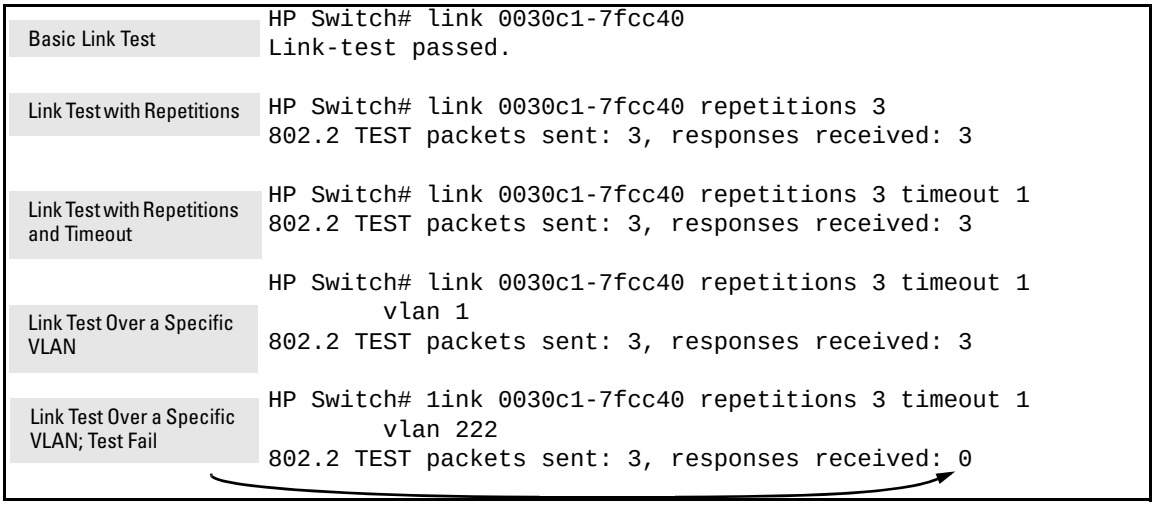



**Figure C-17. Example of Link Tests**

## Traceroute Command

The **traceroute** command enables you to trace the route from the switch to a host address.

This command outputs information for each (router) hop between the switch and the destination address. Note that every time you execute **traceroute**, it uses the same default settings unless you specify otherwise for that instance of the command.

***Syntax:*** traceroute < ip-address | hostname >
traceroute6 < ip-address | hostname >

*Lists the IP address or hostname of each hop in the route, plus the time in microseconds for the* **traceroute** *packet reply to the switch for each hop.*

*To halt an ongoing traceroute search, press the* **[Ctrl] [C]** *keys.*

***Note****: For information about* **traceroute6**, *see the "IPv6 Configuration Guide" for your switch.*

<ip-address | hostname>

*The IP address or hostname of the device to which to send the traceroute.*

[minttl < 1-255 >]

*For the current instance of* **traceroute**, *changes the minimum number of hops allowed for each probe packet sent along the route. If* **minttl** *is greater than the actual number of hops, then the output includes only the hops at and above the* **minttl** *threshold. (The hops below the threshold are not listed.) If* **minttl** *matches the actual number of hops, only that hop is shown in the output. If* **minttl** *is less than the actual number of hops, then all hops are listed. For any instance of* **traceroute,** *if you want a* **minttl** *value other than the default, you must specify that value. (Default: 1)*

[maxttl < 1-255 >]

*For the current instance of* **traceroute**, *changes the maximum number of hops allowed for each probe packet sent along the route. If the destination address is further from the switch than* **maxttl** *allows, then* **traceroute** *lists the IP addresses for all hops it detects up to the* **maxttl** *limit. For any instance of* **traceroute,** *if you want a* **maxttl** *value other than the default, you must specify that value. (Default: 30)*

[timeout < 1-120 >]

*For the current instance of* **traceroute**, *changes the timeout period the switch waits for each probe of a hop in the route. For any instance of* **traceroute,** *if you want a* **timeout** *value other than the default, you must specify that value. (Default: 5 seconds)*

[probes < 1-5 >]

*For the current instance of* **traceroute**, *changes the number of queries the switch sends for each hop in the route. For any instance of* **traceroute,** *if you want a* **probes** *value other than the default, you must specify that value. (Default: 3)*

[source <ip-addr | vlan-id>]

*The source IP address or VLAN. The source IP address must be owned by the router. If a VLAN is specified, the IP address associated with the specified VLAN is used*

**A Low Maxttl Causes Traceroute To Halt Before Reaching the Destination Address.** For example, executing **traceroute** with its default values for a destination IP address that is four hops away produces a result similar to this:

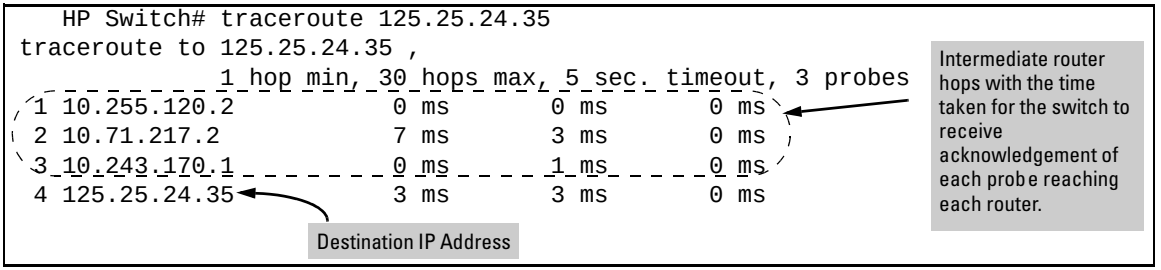



**Figure C-18. Example of a Completed Traceroute Enquiry**

Continuing from the previous example (Figure C-18, above), executing **traceroute** with an insufficient **maxttl** for the actual hop count produces an output similar to this:

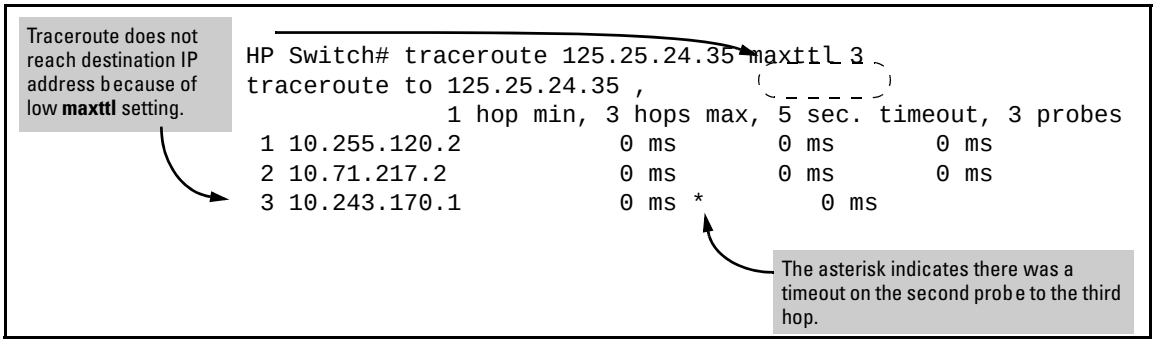



**Figure C-19. Example of Incomplete Traceroute Due to Low Maxttl Setting**

**If A Network Condition Prevents Traceroute from Reaching the Destination.** Common reasons for Traceroute failing to reach a destination include:

- Timeouts (indicated by one asterisk per probe, per hop; refer to Figure C-19, above.)
- Unreachable hosts
- Unreachable networks
- Interference from firewalls
- Hosts configured to avoid responding

Executing traceroute where the route becomes blocked or otherwise fails results in an output marked by timeouts for all probes beyond the last detected hop. For example with a maximum hop count of 7 (**maxttl** = 7), where the route becomes blocked or otherwise fails, the output appears similar to this:

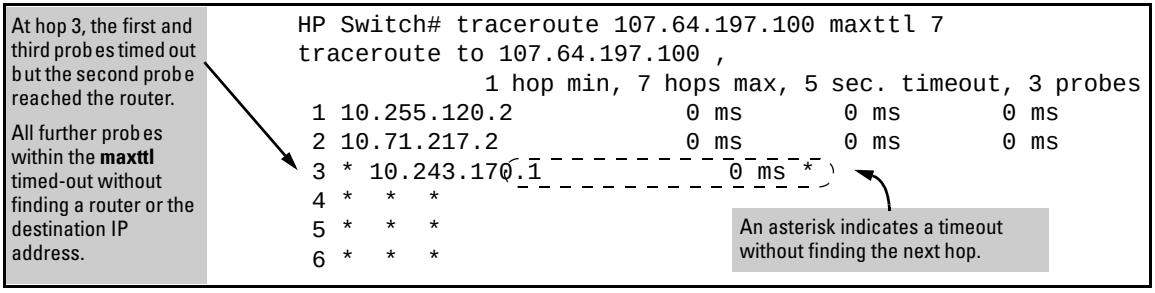



**Figure C-20. Example of Traceroute Failing to Reach the Destination Address**

# Viewing Switch Configuration and Operation

In some troubleshooting scenarios, you may need to view the switch configuration to diagnose a problem. The complete switch configuration is contained in a file that you can browse from either the web browser interface or the CLI using the commands described in this section.

## CLI: Viewing the Startup or Running Configuration File

Using the CLI, you can display either the running or the startup configuration. For more information and examples of how to use these commands, refer to *Getting Started Guide*.)

***Syntax:*** write terminal

*Displays the running configuration.*

show config

*Displays the startup configuration.*

show running-config

*Displays the running-config file.*

## Web: Viewing the Configuration File

To display the running configuration, through the web browser interface:

1. Click on the **Diagnostics** tab.
2. Click on **[Configuration Report]**
3. Use the right-side scroll bar to scroll through the configuration listing.

## CLI: Viewing a Summary of Switch Operational Data

***Syntax:*** show tech

By default, the **show tech** command displays a single output of switch operating and running-configuration data from several internal switch sources, including:

- Image stamp (software version data)
- Running configuration
- Event Log listing
- Boot History
- Port settings
- Status and counters — port status
- IP routes
- Status and counters — VLAN information
- GVRP support
- Load balancing (trunk and LACP)

Figure C-21 shows sample output from the **show tech** command.

```
HP Switch# show tech
show system
 Status and Counters - General System Information
  System Name        : Switch
  MAC Age Time (sec) : 300
  Time Zone          : 0
  Daylight Time Rule : None
  Software revision  : YA.15.XX         Base MAC Addr      : 001871-c42f00
  ROM Version        : YA.15.01         Serial Number      : SG641SU00L
  Up Time            : 23 hours         Memory   - Total   :
  CPU Util (%)       : 10                          Free    :
  IP Mgmt  - Pkts Rx : 759              Packet   - Total   : 6750
             Pkts Tx : 2                Buffers    Free    : 5086
                                                   Lowest  : 4961
                                                   Missed  : 0
```

**Figure C-21. Example of Show Tech Command**

## Saving show tech Command Output to a Text File

When you enter the **show tech** command, a summary of switch operational data is sent to your terminal emulator. You can use your terminal emulator's text capture features to save the **show tech** data to a text file for viewing, printing, or sending to an associate to diagnose a problem.

For example, if your terminal emulator is the Hyperterminal application available with Microsoft® Windows® software, you can copy the **show tech** output to a file and then use either Microsoft Word or Notepad to display the data. (In this case, Microsoft Word provides the data in an easier-to-read format.)

The following example uses the Microsoft Windows terminal emulator. If you are using a different terminal emulator application, refer to the documentation provided with the application.

To save **show tech** command output from your terminal emulator to a text file, follow these steps:

1. In Hyperterminal, click on **Transfer | Capture Text...**

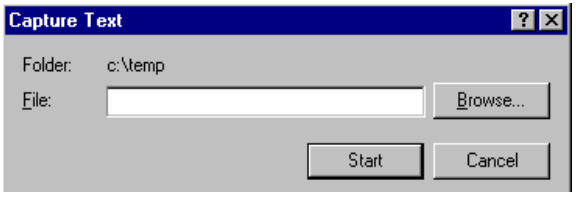



**Figure C-22. Capture Text window of the Hyperterminal Application**

2. In the **File** field, enter the path and file name in which you want to store the **show tech** output.

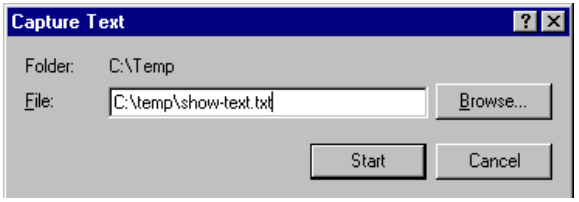



**Figure C-23. Entering a Path and Filename for Saving show tech Output**

3. Click **[Start]** to create and open the text file.
4. From the global configuration context, enter the **show tech** command:

```
HP Switch# show tech
```

The **show tech** command output is copied into the text file and displayed on the terminal emulator screen. When the command output stops and displays -- MORE --, press the Space bar to display and copy more information. The CLI prompt appears when the command output finishes.

5. Click on **Transfer | Capture Text | Stop** in HyperTerminal to stop copying data and save the text file.

   If you do not stop HyperTerminal from copying command output into the text file, additional unwanted data can be copied from the HyperTerminal screen.

6. To access the file, open it in Microsoft Word, Notepad, or a similar text editor.

## CLI: Viewing More Information on Switch Operation

Use the following commands to display additional information on switch operation for troubleshooting purposes.

***Syntax:*** show boot-history

*Displays the boot system log.*

show history

*Displays the current command history. This command output is used for reference or when you want to repeat a command.*

show system-information

*Displays globally configured parameters and information on switch operation (see "CLI: Viewing and Configuring System Information" in the "Interface Access and System Information" chapter).*

show version

*Displays the software version currently running on the switch, and the flash image from which the switch booted (primary or secondary). For more information, see "Displaying Management Information" in the "Redundancy (Switch 8212zl)" chapter.*

show interfaces

*Displays information on the activity on all switch ports (see "CLI: Viewing Port Status and Configuring Port Parameters" in the "Port Status and Configuration" chapter).*

***Syntax:*** show boot-history

show interfaces-display

*Displays summary of the network traffic handled by the ports.*

*Displays the same information as the* **show interfaces** *command and dynamically updates the output every three seconds. Press Ctrl + C to stop the dynamic updates of system information. Use the Arrow keys to view information that is off the screen.*

## Pattern Matching When Using the Show Command

The pattern matching option with the **show** command provides the ability to do searches for specific text. Selected portions of the output are displayed depending on the parameters chosen.

***Syntax:*** show <*command option*> | <include | exclude | begin > <regular expression>

*Use matching pattern searches to display selected portions of the output from a* ***show*** *command. There is no limit to the number of characters that can be matched. Only regular expressions are permitted; symbols such as the asterisk cannot be substituted to perform more general matching.*

**include** *Only the lines that contain the matching pattern are displayed in the output.*

**exclude***: Only the lines that contain the matching pattern are not displayed in the output.*

**begin:** *The display of the output begins with the line that contains the matching pattern.*

**Note**

Pattern matching is case-sensitive.

Below are examples of what portions of the running config file display depending on the option chosen.

```
HP Switch(config)# show run | include ipv6
   ipv6 enable
   ipv6 enable
ipv6 access-list "EH-01"
HP Switch(config)#
```

Displays only lines that contain “ipv6”.

**Figure C-24. Example of Pattern Matching with Include Option**

```
HP Switch(config)# show run | exclude ipv6

Running configuration:

; J9299A Configuration Editor; Created on release #YA.15.XX
; Ver #01:01:00

hostname "HP-2520G-24-PoE"
mirror-port 4
qos dscp-map 000000 priority 0
qos dscp-map 001000 priority 1
...
interface 1
   lacp Active
exit
interface 6
   name "Print_Server"
exit
...
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
   exit
...
port-security 17 learn-mode static address-limit 3 action send-alarm
power-over-ethernet pre-std-detect
no ip ssh cipher 3des-cbc
ip timep dhcp
snmp-server community "public" unrestricted
snmp-server community "public" unrestricted
...
vlan 1
   exit
```

Displays all lines that don't contain "ipv6".

**Figure C-25. Example of Pattern Matching with Exclude Option**

```
HP Switch(config)# show run | begin ipv6
   ipv6 enable
   no untagged 21-24
   exit
vlan 20
   name "VLAN20"
   untagged 21-24
   ipv6 enable
   no ip address
   exit
policy qos "michael"
   exit
ipv6 access-list "EH-01"
   sequence 10 deny tcp 2001:db8:255::/48 2001:db8:125::/48
   exit
no autorun
password manager
```

Displays the running config beginning at the first line that contains "ipv6".

**Figure C-26. Example of Pattern Matching with Begin Option**

Figure C-27 is an example of the **show arp** command output, and then the output displayed when the **include** option has the IP address of **12.255.128.1** as the regular expression.

```
HP Switch(config)# show arp

 IP ARP table

  IP Address       MAC Address       Type    Port
  ---------------  ----------------- ------- ----
  12.255.128.1     00000c-07ac00     dynamic 1
  12.255.131.19    00a0c9-b1503d     dynamic
  12.255.133.150   000bcd-3cbeec     dynamic 1


HP Switch(config)# show arp | include 12.255.128.1
  12.255.128.1     00000c-07ac00     dynamic 1
```

**Figure C-27. Example of the Show ARP Command and Pattern Matching with the Include Option**

# CLI: Useful Commands for Troubleshooting Sessions

Use the following commands in a troubleshooting session to more accurately display the information you need to diagnose a problem. For more information on other these CLI practices, refer to chapter *Getting Started Guide*.

***Syntax:*** alias

*Creates a shortcut alias name for commonly used commands and command options.*

*For more information, see "Using a Command Alias" in the "Using the Command Line Interface (CLI)" chapter.*

***Syntax:*** alias

*Creates a shortcut alias name for commonly used commands and command options.*

*For more information, see "*Getting Started Guide*" in the "Using the Command Line Interface (CLI)" chapter.*

kill

*Terminates a currently running, remote troubleshooting session. Use the* **show ip ssh command** *to list the current management sessions.*

*For more information, see "Denying Interface Access by Terminating Remote Management Sessions" in the "Interface Access and System Information" chapter.*

[no] page

*Toggles the paging mode for* **show** *commands between continuous listing and per-page listing.*

repeat

*Repeatedly executes one or more commands so that you can see the results of multiple commands displayed over a period of time. To halt the command execution, press any key on the keyboard.*

*For more information, see "Repeating a Command" in the "Using the Command Line Interface (CLI)" chapter.*

setup

*Displays the Switch Setup screen from the menu interface.*

# Restoring the Factory-Default Configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process momentarily interrupts the switch operation, clears any passwords, clears the console Event Log, resets the network counters to zero, performs a complete self test, and reboots the switch into its factory default configuration including deleting an IP address. There are two methods for resetting to the factory-default configuration:

- CLI
- Clear/Reset button combination

**Note** HPrecommends that you save your configuration to a TFTP server before resetting the switch to its factory-default configuration. You can also save your configuration via Xmodem, to a directly connected PC.

## CLI: Resetting to the Factory-Default Configuration

This command operates at any level *except* the Operator level.

***Syntax:*** erase startup-configuration

*Deletes the startup-config file in flash so that the switch will reboot with its factory-default configuration.*

**Note** The **erase startup-config** command does not clear passwords.

## Clear/Reset: Resetting to the Factory-Default Configuration

To execute the factory default reset, perform these steps:

1. Using pointed objects, simultaneously press both the Reset and Clear buttons on the front of the switch.

2. Continue to press the Clear button while releasing the Reset button.
3. When the Self Test LED begins to flash, release the Clear button.

   The switch will then complete its self test and begin operating with the configuration restored to the factory default settings.

# Restoring a Flash Image

The switch can lose its operating system if either the primary or secondary flash image location is empty or contains a corrupted OS file and an operator uses the **erase flash** command to erase a good OS image file from the opposite flash location.

**To Recover from an Empty or Corrupted Flash State.** Use the switch's console serial port to connect to a workstation or laptop computer that has the following:

- A terminal emulator program with Xmodem capability, such as the HyperTerminal program included in Windows PC software.
- A copy of a good OS image file for the switch.

**Note**

The following procedure requires the use of Xmodem, and copies an OS image into primary flash only.

This procedure assumes you are using HyperTerminal as your terminal emulator. If you use a different terminal emulator, you may need to adapt this procedure to the operation of your particular emulator.

1. Start the terminal emulator program.
2. Ensure that the terminal program is configured as follows:

   - Baud rate: 9600
   - No parity
   - 8 Bits
   - 1 stop bit
   - No flow control

3. Use the Reset button to reset the switch. The following prompt should then appear in the terminal emulator:

```
Enter h or ? for help.

=>
```

4. Since the OS file is large, you can increase the speed of the download by changing the switch console and terminal emulator baud rates to a high speed. For example:
   a. Change the switch baud rate to 115,200 Bps.

```
=> sp 115200
```

   b. Change the terminal emulator baud rate to match the switch speed:
      i. In HyperTerminal, select **Call** | **Disconnect**.
      ii. Select **File** | **Properties**.
      iii. Click on **Configure.**
      iv. Change the baud rate to **115200**.
      v. Click on **[OK]**. In the next window, click on **[OK]** again.
      vi. Select **Call** | **Connect**
      vii. Press **[Enter]** one or more times to display the => prompt.

5. Start the Console Download utility by typing **do** at the => prompt and pressing **[Enter]**:

```
=> do
```

6. You will then see this prompt:

```
You have invoked the console download utility.
Do you wish to continue? (Y/N)>_
```

7. At the above prompt:
   a. Type **y** (for Yes)
   b. Select **Transfer** | **File** in HyperTerminal.
   c. Enter the appropriate filename and path for the OS image.
   d. Select the **Xmodem** protocol (and not the 1k Xmodem protocol).
   e. Click on **[Send]**.

   If you are using HyperTerminal, you will see a screen similar to the following to indicate that the download is in progress:

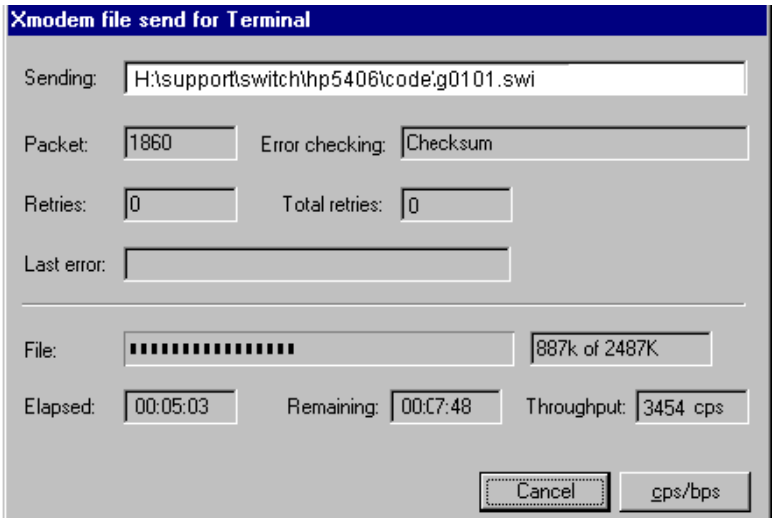



**Figure C-28. Example of Xmodem Download in Progress**

8. When the download completes, the switch reboots from primary flash using the OS image you downloaded in the preceding steps, plus the most recent startup-config file.

# DNS Resolver

The Domain Name System (DNS) resolver is designed for use in local network domains where it enables use of a host name or fully qualified domain name with DNS-compatible switch CLI commands.

DNS operation supports both IPv4 and IPv6 DNS resolution and multiple, prioritized DNS servers. (For information on IPv6 DNS resolution, refer to the latest *IPv6 Configuration Guide* for your switch.)

## Terminology

**Domain Suffix —** Includes all labels to the right of the unique host name in a fully qualified domain name assigned to an IP address. For example, in the fully qualified domain name “device53.evergreen.trees.org”, the domain suffix is “evergreen.trees.org”, while “device53” is the unique (host) name assigned to a specific IP address.

**Fully Qualified Domain Name —** The sequence of labels in a domain name identifying a specific host (host name) and the domain in which it exists. For example, if a device with an IP address of 10.10.10.101 has a host name of *device53* and resides in the *evergreen.trees.org* domain, then the device's fully qualified domain name is *device53.evergreen.trees.org* and the DNS resolution of this name is 10.10.10.101.

**Host Name —** The unique, leftmost label in a domain name assigned to a specific IP address in a DNS server configuration. This enables the server to distinguish a device using that IP address from other devices in the same domain. For example, in the *evergreen.trees.org* domain, if an IPv4 address of 10.10.100.27 is assigned a host name of *accounts015* and another IP address of 10.10.100.33 is assigned a host name of *sales021*, then the switch configured with the domain suffix *evergreen.trees.org* and a DNS server that resolves addresses in that domain can use the host names to reach the devices with DNS-compatible commands. For example:

```
ping accounts015
traceroute accounts015
```

## Basic Operation

- When the switch is configured with only the IP address of a DNS server available to the switch, then a DNS-compatible command, executed with a fully qualified domain name, can reach a device found in any domain accessible through the configured DNS server.
- When the switch is configured with both of the following:
  - the IP address of a DNS server available to the switch
  - the domain suffix of a domain available to the configured DNS server

  then:
  - A DNS-compatible command that includes the host name of a device in the same domain as the configured domain suffix can reach that device.
  - A DNS-compatible command that includes a fully qualified domain name can reach a device in any domain that is available to the configured DNS server.

**Example.** Suppose the switch is configured with the domain suffix **mygroup.networking.net** and the IP address for an accessible DNS server. If an operator wants to use the switch to ping a target host in this domain by using

the DNS name "leader" (assigned by a DNS server to an IP address used in that domain), then the operator can use either of the following commands:

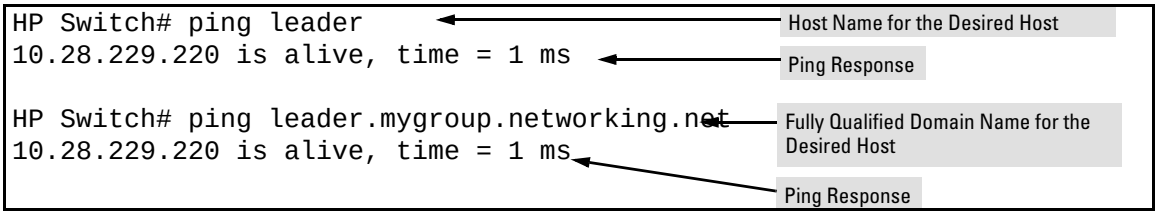



**Figure C-29. Example of Using Either a Host Name or a Fully Qualified Domain Name**

In the proceeding example, if the DNS server's IP address is configured on the switch, but a domain suffix is either not configured or is configured for a different domain than the target host, then the fully qualified domain name *must* be used.

Note that if the target host is in a domain *other than* the domain configured on the switch, then:

- The host's domain must be reachable from the switch. This requires that the DNS server for the switch must be able to communicate with the DNS server(s) in the path to the domain in which the target host operates.
- The fully qualified domain name must be used, and the domain suffix must correspond to the domain in which the target host operates, regardless of the domain suffix configured in the switch.

**Example.** Suppose the switch is configured with the domain suffix **mygroup.networking.net** and the IP address for an accessible DNS server in this same domain. This time, the operator wants to use the switch to trace the route to a host named "remote-01" in a different domain named **common.group.net**. Assuming this second domain is accessible to the DNS server already configured on the switch, a **traceroute** command using the target's fully qualified DNS name should succeed.

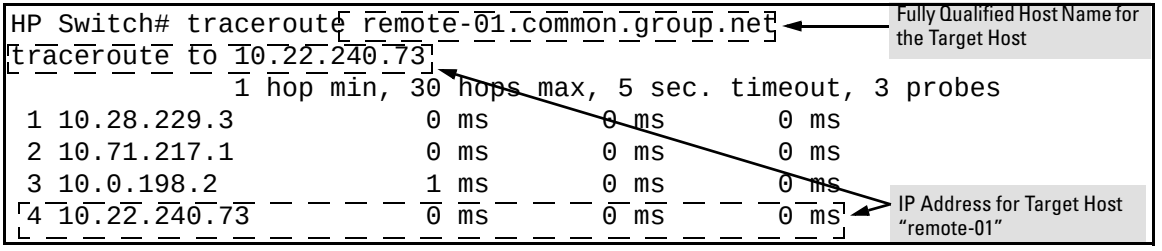



**Figure C-30. Example Using the Fully Qualified Domain Name for an Accessible Target in Another Domain**

## Configuring and Using DNS Resolution with DNS-Compatible Commands

1. Determine the following:
   a. The IP address for a DNS server operating in a domain in your network
   b. The priority (1 - 3) of the selected server, relative to other DNS servers in the domain
   c. The domain name for an accessible domain in which there are hosts you want to reach with a DNS-compatible command. (This is the domain suffix in the fully qualified domain name for a given host operating in the selected domain. Refer to "Terminology" on page C-63.) Note that if a domain suffix is not configured, fully qualified domain names can be used to resolve DNS-compatible commands.
   d. the host names assigned to target IP addresses in the DNS server for the specified domain
2. Use the data from steps 1a through 1c to configure the DNS entry on the switch.
3. Use a DNS-compatible command with the host name to reach the target devices.

## Configuring a DNS Entry

The switch allows up to three DNS server entries (IP addresses for DNS servers). One domain suffix can also be configured to support resolution of DNS names in that domain by using a host name only. Including the domain suffix enables the use of DNS-compatible commands with a target's host name instead of the target's fully qualified domain name.

***Syntax:*** [no] ip dns server-address priority < 1 - 3 > < *ip-addr* >

*Configures the access priority and IP address of a DNS server accessible to the switch. These settings specify:*

- *the relative priority of the DNS server when multiple servers are configured*
- *the IP address of the DNS server*

*These settings must be configured before a DNS-compatible command can be executed with host name criteria.*

*The switch supports three prioritized DNS server entries. Configuring another IP address for a priority that has already been assigned to an IP address is not allowed. To replace one IP address at a given priority level with another address having the same priority, you must first use the* **no** *form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed. To change the priority of an existing server address, use the* **no** *form of the command to remove the entry, then re-enter the address with the new priority.*

*The* **no** *form of the command replaces the configured IP address with the null setting. (Default: null)*

***Syntax:*** [no] ip dns domain-name < *domain-name-suffix* >

*This optional DNS command configures the domain suffix that is automatically appended to the host name entered with a DNS-compatible command. When the domain suffix and the IP address for a DNS server that can access that domain are both configured on the switch, you can execute a DNS-compatible command using only the host name of the desired target. (For an example, refer to Figure C-29 on page C-65.) In either of the following two instances, you must manually provide the domain identification by using a fully qualified DNS name with a DNS-compatible command:*

- *If the DNS server IP address is configured on the switch, but the domain suffix is not configured (null)*
- *The domain suffix configured on the switch is not the domain in which the target host exists*

*The switch supports one domain suffix entry and three DNS server IP address entries. (Refer to the preceding command description.)*

*The* **no** *form of the command replaces the configured domain suffix with the null setting. (Default: null)*

## Example Using DNS Names with Ping and Traceroute

In the network illustrated in Figure C-31, the switch at 10.28.192.1 is configured to use DNS names for DNS-compatible commands in the *pubs.outdoors.com* domain. The DNS server has been configured to assign the host name *docservr* to the IP address used by the document server (10.28.229.219).

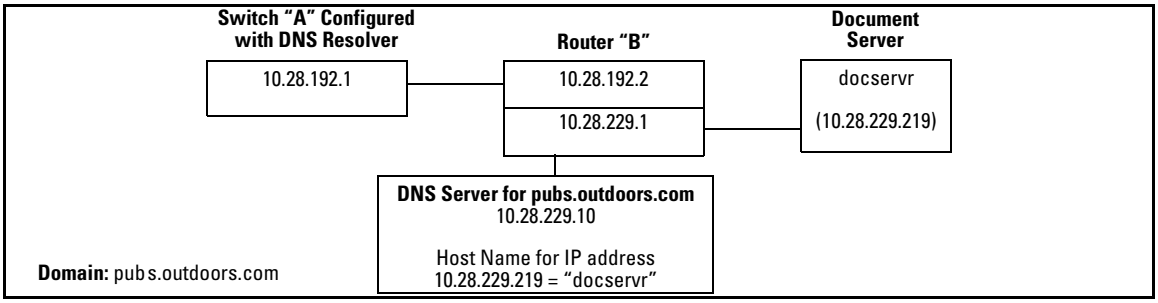



**Figure C-31. Example Network Domain**

Configuring switch "A" with the domain name and the IP address of a DNS server for the domain enables the switch to use host names assigned to IP addresses in the domain to perform **ping** and **traceroute** actions on the devices in the domain. To summarize:

| Entity: | Identity: |
|---|---|
| DNS Server IP Address | 10.28.229.10 |
| Domain Name (and Domain Suffix for Hosts in the Domain) | pubs.outdoors.com |
| Host Name Assigned to 10.28.229.219 by the DNS Server | docservr |
| Fully Qualified Domain Name for the IP address Used By the Document Server (10.28.229.219) | docservr.pubs.outdoors.com |
| Switch IP Address | 10.28.192.1 |
| Document Server IP Address | 10.28.229.219 |

With the above already configured, the following commands enable a DNS-compatible command with the host name **docserver** to reach the document server at 10.28.229.219.

```
HP Switch(config)# ip dns server-address 10.28.229.10
HP Switch(config)# ip dns domain-name pubs.outdoors.com
```

**Figure C-32. Configuring Switch "A" in FigureC-31 To Support DNS Resolution**

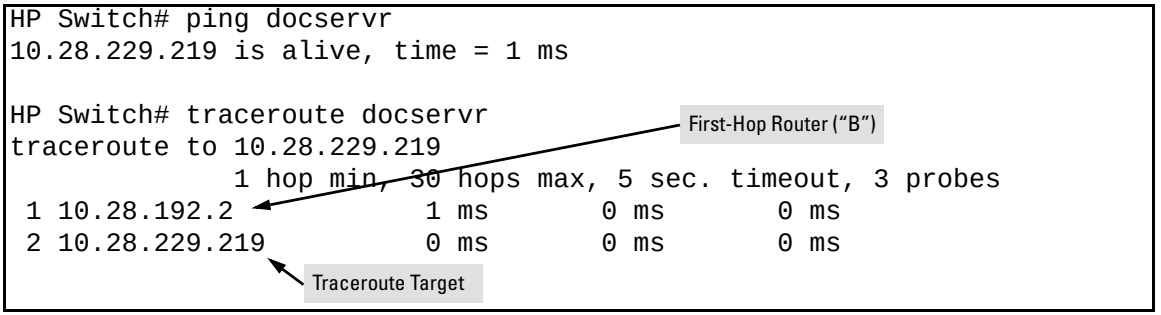



**Figure C-33. Example of Ping and Traceroute Execution for the Network in Figure C-31 on Page C-68**

As mentioned under "Basic Operation" on page C-64, if the DNS entry configured in the switch does not include the domain suffix for the desired target, then you must use the target host's fully qualified domain name with DNS-compatible commands. For example, using the document server in Figure C-31 as a target:

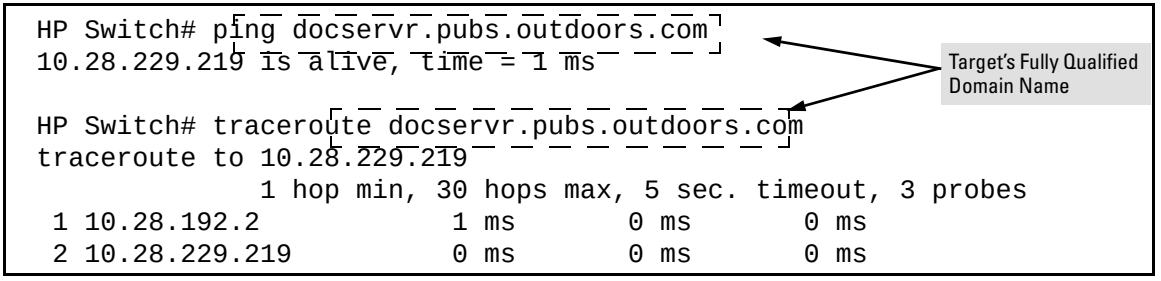



**Figure C-34. Example of Ping and Traceroute Execution When Only the DNS Server IP Address Is Configured**

## Viewing the Current DNS Configuration

The **show ip** command displays the current domain suffix and the IP address of the highest priority DNS server configured on the switch, along with other IP configuration information. If the switch configuration currently includes a non-default (non-null) DNS entry, it will also appear in the **show run** command output.

```
HP Switch# show ip

 Internet (IP) Service

  Default Gateway : 10.28.192.2
  Default TTL     : 64
  Arp Age         : 20
  Domain Suffix   : pubs.outdoors.com
  DNS server      : 10.28.229.10
 ┌─────────────────────────────────┐
 │VLAN         | IP Config  IP Address  │  Subn
 └─────────────┼─────────────────────────┘
  DEFAULT_VLAN | Manual     10.28.192.1     255.255.255.0
```

DNS Resolver Configuration in the **show ip** command output

**Figure C-35. Example of Viewing the Current DNS Configuration**

## Operating Notes

- Configuring another IP address for a priority that has already been assigned to an IP address is not allowed. To replace one IP address at a given priority level with another address having the same priority, you must first use the **no** form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed. To change the priority of an existing server address, use the **no** form of the command to remove the entry, then re-enter the address with the new priority.
- To change the position of an address already configured with priority x, you must first use **no ip dns server-address priority x < *ip-addr* >** to remove the address from the configuration, then use **ip dns server-address priority < *ip-addr* >** to reconfigure the address with the new priority. Also, if the priority to which you want to move an address is already used in the configuration for another address, you must first use the no form of the command to remove the current address from the target priority.
- The DNS server(s) and domain configured on the switch must be accessible to the switch, but it is not necessary for any intermediate devices between the switch and the DNS server to be configured to support DNS operation.
- When multiple DNS servers are configured on the switch, they can reside in the same domain or different domains.

- A DNS configuration must include the IP address for a DNS server that is able to resolve host names for the desired domain. If a DNS server has limited knowledge of other domains, then its ability to resolve DNS-compatible command requests is also limited.
- If the DNS configuration includes a DNS server IP address but does not also include a domain suffix, then any DNS-compatible commands should include the target host's fully qualified domain name. Refer to Figure C-29 on page C-65.
- Switch-Initiated DNS packets go out through the VLAN having the best route to the DNS server, even if a Management VLAN has been configured.
- The DNS server address must be manually input. It is not automatically determined via DHCP.

## Event Log Messages

| Message | Meaning |
|---|---|
| DNS server address not configured | The switch does not have an IP address configured for the DNS server. |
| DNS server not responding | The DNS server failed to respond or is unreachable. An incorrect server IP address can produce this result. |
| Unknown host < *host-name* > | The host name did not resolve to an IP address. Some reasons for this occurring include:<br>• The host name was not found.<br>• The named domain was not found.<br>• The domain suffix was expected, but has not been configured. (If the server's IP address has been configured in the switch but the domain name has not been configured, then the host's fully qualified domain name must be used.) |

# MAC Address Management

The switch assigns MAC addresses in these areas:

- For management functions, one Base MAC address is assigned to the default VLAN (VID = 1). (All VLANs on the switches covered in this guide use the same MAC address.)
- For internal switch operations: One MAC address per port (Refer to "CLI: Viewing the Port and VLAN MAC Addresses" on page D-3.)

MAC addresses are assigned at the factory. The switch automatically implements these addresses for VLANs and ports as they are added to the switch.

**Note** The switch's base MAC address is also printed on a label affixed to the switch.

## Determining MAC Addresses

**MAC Address Viewing Methods**

| Feature | Default | Menu | CLI | Web |
|---|---|---|---|---|
| view switch's base (default vlan) MAC address and the addressing for any added VLANs | n/a | D-2 | D-3 | — |
| view port MAC addresses (hexadecimal format) | n/a | — | D-3 | — |

- **Use the menu interface** to view the switch's base MAC address and the MAC address assigned to any VLAN you have configured on the switch. (The same MAC address is assigned to VLAN1 and all other VLANs configured on the switch.)

**Note** The switch's base MAC address is used for the default VLAN (VID = 1) that is always available on the switch. This is true for dynamic VLANs as well; the base MAC address is the same across all VLANs.

- **Use the CLI** to view the switch's port MAC addresses in hexadecimal format.

## Menu: Viewing the Switch's MAC Addresses

The Management Address Information screen lists the MAC addresses for:

- Base switch (default VLAN; VID = 1)
- Any additional VLANs configured on the switch.

Also, the Base MAC address appears on a label on the back of the switch.

**Note**

The Base MAC address is used by the first (default) VLAN in the switch. This is usually the VLAN named "DEFAULT_VLAN" unless the name has been changed (by using the VLAN Names screen). On the switches covered in this guide, the VID (VLAN identification number) for the default VLAN is always "1", *and cannot be changed.*

**To View the MAC Address (and IP Address) assignments for VLANs Configured on the Switch:**

1. From the Main Menu, Select

   **1. Status and Counters**

   **2. Switch Management Address Information**

   If the switch has only the default VLAN, the following screen appears. If the switch has multiple static VLANs, each is listed with its address data.

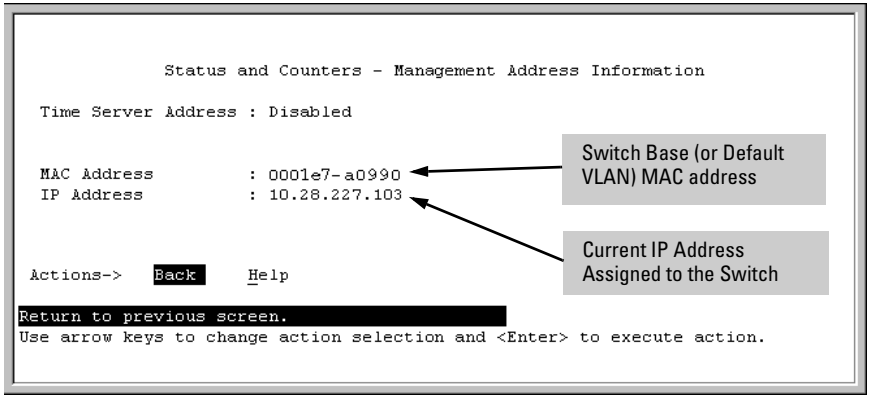



**Figure D-1. Example of the Management Address Information Screen**

## CLI: Viewing the Port and VLAN MAC Addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control and the spanning-tree protocol. Using the **walkmib** command to determine the MAC address assignments for individual ports can sometimes be useful when diagnosing switch operation.

The switch's base MAC address is assigned to VLAN (VID) 1 and appears in the **walkmib** listing after the MAC addresses for the ports. (All VLANs in the switch have the same MAC address.)

To display the switch's MAC addresses, use the **walkmib** command at the command prompt:

**Note**

This procedure displays the MAC addresses for all ports and existing VLANs in the switch, regardless of which VLAN you select.

1. If the switch is at the CLI Operator level, use the **enable** command to enter the Manager level of the CLI.
2. Type the following command to display the MAC address for each port on the switch:

   ```
   HP Switch# walkmib ifPhysAddress
   ```

   (The above command is not case-sensitive.)

```
HP Switch(config)# walkmib ifphysaddress
ifPhysAddress.1 = 00 1f fe 74 b3 ff
ifPhysAddress.2 = 00 1f fe 74 b3 fe
ifPhysAddress.3 = 00 1f fe 74 b3 fd
ifPhysAddress.4 = 00 1f fe 74 b3 fc
ifPhysAddress.5 = 00 1f fe 74 b3 fb
ifPhysAddress.6 = 00 1f fe 74 b3 fa
ifPhysAddress.7 = 00 1f fe 74 b3 f9
ifPhysAddress.8 = 00 1f fe 74 b3 f8
ifPhysAddress.9 = 00 1f fe 74 b3 f7
ifPhysAddress.10 = 00 1f fe 74 b3 f6
ifPhysAddress.58 = 00 1f fe 74 b3 e0
ifPhysAddress.313 = 00 1f fe 74 b3 e0
ifPhysAddress.314 = 00 1f fe 74 b3 e0
ifPhysAddress.4150 = 00 1f fe 74 b3 e0
ifPhysAddress.4151 = 00 1f fe 74 b3 e0
```

**Figure B-5. Example of Port MAC Address Assignments on a Switch**

# Viewing the MAC Addresses of Connected Devices

***Syntax:*** show mac-address [ | *mac-addr* |

*Lists the MAC addresses of the devices the switch has detected, along with the number of the specific port on which each MAC address was detected.*

[ *port-list* ]

*Lists the MAC addresses of the devices the switch has detected, on the specified port(s).*

[ *mac-addr* ]

*Lists the port on which the switch detects the specified MAC address. Returns the following message if the specified MAC address is not detected on any port in the switch:*

`MAC address <mac-addr> not found.`

[ vlan < *vid* > ]

*Lists the MAC addresses of the devices the switch has detected on ports belonging to the specified VLAN, along with the number of the specific port on which each MAC address was detected.*

To list the MAC addresses of devices the switch has detected, use the **show mac-address** command.

```
HP Switch(config)# show mac-address

 Status and Counters - Port Address Table

  MAC Address   Located on Port
  ------------- ---------------
  00000c-07ac00 1
```

**Figure B-6. Example of show mac-address Command**

# Daylight Savings Time on HP Switches

This information applies to the following HP switches:

- 212M
- 224M
- 1600M
- 2400M
- 2424M
- 4000M
- 8000M
- Series 2500
- Series 2520
- Series 2600
- Series 2800
- Series 2900
- Series 2910al
- Series 3400cl
- Series 3500
- Series 3500yl
- Series 4100gl
- Series 4200vl
- Series 5300xl
- Series 5400zl
- Switch 6108
- Switch 6200yl
- Series 6400cl
- Series 6600
- Series 8200zl
- HP AdvanceStack Switches
- HP AdvanceStack Routers

HP switches provide a way to automatically adjust the system clock for Daylight Savings Time (DST) changes. To use this feature you define the month and date to begin and to end the change from standard time. In addition to the value “none” (no time changes), there are five pre-defined settings, named:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The pre-defined settings follow these rules:

**Alaska:**

- Begin DST at 2am on the second Sunday in March.
- End DST at 2am on the first Sunday in November.

**Canada and Continental US:**

- Begin DST at 2am on the second Sunday in March.
- End DST at 2am on the first Sunday in November.

**Middle Europe and Portugal:**

- Begin DST at 2am the first Sunday on or after March 25th.
- End DST at 2am the first Sunday on or after September 24th.

**Southern Hemisphere:**

- Begin DST at 2am the first Sunday on or after October 25th.
- End DST at 2am the first Sunday on or after March 1st.

**Western Europe:**

- Begin DST at 2am the first Sunday on or after March 23rd.
- End DST at 2am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows you to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change. The menu interface screen looks like this (all month/date entries are at their default values):

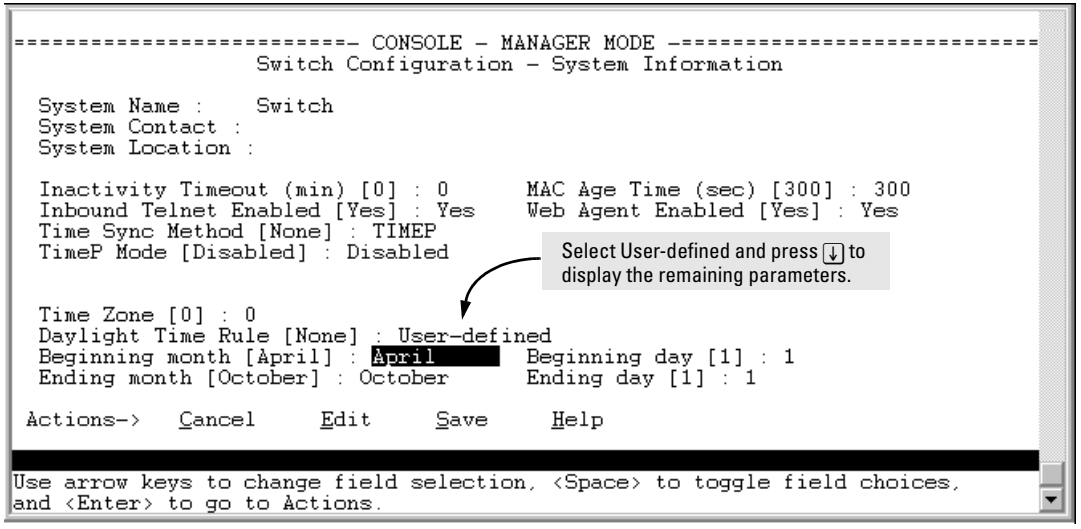



**Figure E-1. Menu Interface with "User-Defined" Daylight Time Rule Option**

Before configuring a “User defined” Daylight Time Rule, it is important to understand how the switch treats the entries. The switch knows which dates are Sundays, and uses an algorithm to determine on which date to change the system clock, given the configured “Beginning day” and “Ending day”:

- If the configured day is a Sunday, the time changes at 2am on that day.
- If the configured day is not a Sunday, the time changes at 2am on the first Sunday after the configured day.

This is true for both the “Beginning day” and the “Ending day”.

With that algorithm, one should use the value “1” to represent “first Sunday of the month”, and a value equal to “number of days in the month minus 6" to represent “last Sunday of the month”. This allows a single configuration for every year, no matter what date is the appropriate Sunday to change the clock.

# Power-Saving Features

## Configuring Power-Saving

The **savepower led** command provides the ability to turn off the switch link, mode, and activity LEDs and turn them on again. When power-saving is turned off, it will turn on again automatically after 10 minutes.

***Syntax:*** [no] savepower led

*Turns power-saving option on or off for the LEDs.*

```
HP Switch(config)# savepower led
```

**Figure F-1. Example of Setting savepower led Command**

The **no** form of the **savepower led** command cancels power saving mode and the LEDs are returned to their original state.

To display the configured status of the LED power-saving option, use the **show savepower led** command.

```
HP Switch(config)# show savepower led

 Led Save Power Status: Enabled
```

**Figure F-2. Example of Output for show savepower led Command**

### Configuring the Savepower port-low-pwr Option

The **port-low-pwr** option puts all the ports on the switch into auto low power mode if they are not linked.

***Syntax:*** [no] savepower port-low-pwr

*Puts ports in low power mode.*

When a link is detected, the ports return to normal power mode.

The **no** form of the command puts the ports into normal power mode.

```
HP Switch(config)# savepower port-low-pwr
```

**Figure F-3. Example of savepower port-low-power Command**

To display the status of the power-down feature, use the **show savepower port-low-pwr** command. The output shows if the feature is enabled or not enabled.

```
HP Switch(config)# show savepower port-low-pwr

 Port Save Power Status: Enabled
```

**Figure F-4. Example of Output for show savepower port-low-pwr Command**

# Index

## Symbols

**=> prompt** … C-61

## Numerics

**802.1X**
effect, LLDP … 5-70
LLDP blocked … 5-39
**802.1X access control**
authentication failure, SNMP notification … 5-23
SNMP notification of authentication failure … 5-23

## A

**access**
manager … 5-10
operator … 5-10
**ACL**
debug messages … C-27
**address**
network manager … 5-2
**address table, port** … B-10
**address, network manager** … 5-3
**advertise location** … 5-51
**AES encryption** … 5-6
**alias**
use for troubleshooting … C-59
**allocation, class** … 3-8
**allocation, value** … 3-8
**ARP protection**
SNMP notification … 5-14, 5-23
**asterisk**
meaning in traceroute … C-51
**authentication**
notification messages … 5-14, 5-23
**authentication trap**
*See also* SNMP.
**authorized IP managers**
SNMP, blocking … 5-1
**auto MDI/MDI-X**
configuration, display … 2-19
operation … 2-18, 2-19
port mode, display … 2-19
**Auto-10** … 4-2, 4-5, 4-15
**autonegotiate** … 5-51

## B

**bandwidth**
displaying port utilization … 2-12
**boot ROM console** … A-2
**boot ROM mode** … C-61
**Bootp**
effect of no reply … C-4
**Bootp/DHCP, LLDP** … 5-47
**broadcast limit** … 2-17
**broadcast storm** … 4-2, C-11
**broadcast traffic**
IPX … 2-17
RIP … 2-17

## C

**CDP** … 5-71, 5-72, 5-73, 5-75
**Clear button**
restoring factory default configuration … C-61
**clear logging** … C-24
**CLI**
context level … 2-15
**command line interface**
*See* CLI.
**communities, SNMP** … 5-11
viewing and configuring with the CLI … 5-12
viewing and configuring with the menu … 5-11
**configuration**
copying … A-20
impacts of software download on … A-2
network monitoring … B-17
port … 2-1
port trunk group … 4-1
port, duplex … 2-14
port, speed … 2-14
restoring factory defaults … C-60
SNMP … 5-2, 5-3, 5-9
SNMP communities … 5-11, 5-12
transferring … A-20

trap receivers … 5-16
**configuration file**
browsing for troubleshooting … C-52
**configuration file, multiple**
copy via tftp … A-21
copy via Xmodem … A-22
**console**
measuring network activity … C-4
troubleshooting access problems … C-2
**copy**
command output … A-24
crash data … A-25
crash log … A-26
event log output … A-25
software images … A-19
tftp show-tech … A-21
**copy tftp**
show-tech … A-21
**CPU utilization** … B-3
**cpu utilization data** … B-4
**custom, show tech** … A-22
**customizing, show command output** … 2-8

## D

**date format, events** … C-17
**debug**
compared to event log … C-26
destination, logging … C-28
displaying debug configuration … C-31
forwarding IPv4 messages … C-28
lldp messages … C-28
overview
packet messages … C-28
sending event log messages … C-26
standard event log messages … C-28
using CLI session … C-27
**debug command**
all … C-33
cdp … C-33
configuring debug/Syslog operation … C-29
destination … C-33
destinations … C-27, C-35
event log … C-44
event log as default … C-27
event log messages … C-33
event types supported … C-26
lldp … C-34
operating notes … C-43
show debug … C-31
snmp … C-35
support for "debug" severity on Syslog servers … C-35, C-44
syntax … C-27, C-33
using CLI session … C-35
**debug logging**
LLDP … 5-38
**default settings**
PoE … 3-4
PoE allocation, *usage* … 3-8
UDLD, *disabled* … 2-35
**default trunk type** … 4-8
**DES encryption** … 5-6
**DHCP**
address problems … C-4
effect of no reply … C-4
**DHCP snooping**
SNMP notification … 5-14, 5-23
**DHCP/Bootp, LLDP** … 5-47
**DHCPv6**
debug messages … C-28
**dhcpv6-client** … C-28
**diagnostics tools** … C-44
browsing the configuration file … C-52
displaying switch operation … C-53
ping and link tests … C-45
traceroute … C-49
viewing switch operation … C-52
**DNS**
configuration … C-66, C-68
configuration error … C-71
configuration, viewing … C-69
domain name, fully qualified … C-64, C-65, C-69
domain suffix … C-63
domain-name configuration … C-67
event log messages … C-71
example … C-68
host name … C-64
IPv6 DNS resolution … C-63
operating notes … C-70
ping … C-69
resolver … C-63
resolver operation … C-64
secure management VLAN … C-71
server address, DHCP not used … C-71
server IP address … C-65, C-71

server-address configuration … C-66
three entries supported … C-66
three server entries supported … C-66
traceroute … C-69
VLAN, best route selection … C-71
**documentation**
latest versions … 1-xv
printed in-box publications … 1-xv
release notes … 1-xv
**download**
software … A-17
software using TFTP … A-2
switch-to-switch … A-17
TFTP … A-2
troubleshooting … A-4
Xmodem … A-14
*See also* switch software.
**duplex advertisements** … 5-49
**duplex information, displaying** … 5-64
**duplicate MAC address**
*See* MAC address.
**Dyn1**
*See* LACP.

## E

**Emergency Location Id Number** … 5-33, 5-59
**event log**
clearing entries … C-24
compared to debug/Syslog operation … C-26
debugging by severity level … C-27, C-36
debugging by system module … C-27, C-36
Event Log Message Reference Guide … 1-xv
format, date … C-17
generated by system module … C-18
how to read entries … C-17
listing entries … C-23
losing messages … C-17
navigation … C-22
not affected by debug configuration … C-44
security levels … 5-17
sending event log messages as traps … 5-17
sending messages to Syslog server … C-27
severity level … C-17, C-42
system module … C-42
time format … C-17
UDLD warning messages … 2-39
used for debugging … C-27
used for troubleshooting … C-17
**excessive packets** … 2-27

## F

**facility**
logging … C-27
**factory default configuration**
restoring … C-60
**failure, switch software download** … A-5
**fault-tolerance** … 4-3
**fiber optics, monitoring links** … 2-34
**filter, source-port** … 2-26
**firmware version** … B-3
**flow control**
constraints … 2-15
global … 2-15
jumbo packets … 2-22, 2-26
per-port … 2-15
**flow control, status** … B-7
**flow sampling** … 5-2
**friendly port names**
*See* port names, friendly.

## G

**giant packets** … 2-27

## H

**HP**
Auto-MDIX feature … 2-18
**HP Networking**
switch documentation … 1-xv
**HP, URL** … 5-2

## I

**IEEE 802.1d** … C-10
**IEEE P802.1AB/D9** … 5-38
**IGMP**
host not receiving … C-5
not working … C-5
statistics … B-15
**Inbound Telnet Enabled parameter** … C-3
**informs**
sending to trap receiver … 5-17
SNMP … 5-18

**IP**
duplicate address … C-4
duplicate address, DHCP network … C-4
time server address … 1-8, 1-17
**IP address**
for SNMP management … 5-1
**IP routing**
debug messages … C-27
**IPv6**
debug dhcpv6 messages … C-28
**IPX**
broadcast traffic … 2-17
network number … B-5

## J

**jumbo packets**
configuration … 2-23
excessive inbound … 2-26
flow control … 2-22, 2-26
GVRP operation … 2-22
management VLAN … 2-25
maximum size … 2-21
MTU … 2-21
port adds and moves … 2-22
port speed … 2-22
security concerns … 2-26
standard MTU … 2-22
through non-jumbo ports … 2-27
traffic sources … 2-22
troubleshooting … 2-27
VLAN tag … 2-21
voice VLAN … 2-25

## L

**LACP**
802.1X not allowed … 4-18
active … 4-13
blocked ports … 4-20
CLI access … 4-9
default port operation … 4-17
described … 4-4, 4-15
Dyn1 … 4-5
dynamic … 4-16
enabling dynamic trunk … 4-13
full-duplex required … 4-2, 4-15
IGMP … 4-19
monitoring static trunk … B-18
no half-duplex … 4-21
operation not allowed … C-6
overview of port mode settings … 4-3
passive … 4-13
removing port from active trunk … 4-14
restrictions … 4-18
standby link … 4-16
status, terms … 4-17
STP … 4-19
trunk limit … 4-16
VLANs … 4-19
with 802.1X … 4-18
with port security … 4-19
**limit, broadcast** … 2-17
**link failures**
detecting … 2-34
**link speed, port trunk** … 4-2
**link test** … C-45
**link-change traps** … 5-14, 5-24
**Link-Layer Discovery Protocol**
*See* LLDP.
**LLDP**
802.1D-compliant switch … 5-69
802.1X blocking … 5-39
802.1X effect … 5-70
active port … 5-33
adjacent device … 5-33
advertisement … 5-33
advertisement content … 5-47
advertisement data … 5-63
advertisement, mandatory data … 5-47
advertisement, optional data … 5-48
advertisements, delay interval … 5-44
CDP neighbor data … 5-71
chassis ID … 5-47
chassis type … 5-47
clear statistics counters … 5-67
comparison with CDP data fields … 5-71
configuration options … 5-35
configuring optional data … 5-48
data options … 5-36
data read options … 5-38
data unit … 5-34
debug logging … 5-38
debug messages … C-27, C-28
default configuration … 5-40
DHCP/Bootp operation … 5-39

disable, per-port … 5-46
display neighbor data … 5-65
ELIN … 5-33
enable/disable, global … 5-42
features … 5-32
general operation … 5-35
global counters … 5-67
holdtime multiplier … 5-43
hub, packet-forwarding … 5-35
IEEE P802.1AB/D9 … 5-38
inconsistent value … 5-44
information options … 5-36
invalid frames … 5-68
IP address advertisement … 5-39, 5-70
IP address subelement … 5-47
IP address, DHCP/Bootp … 5-47
IP address, options … 5-47
IP address, version advertised … 5-47
LLDP-aware … 5-33
LLDPDU … 5-34
mandatory TLVs … 5-70
MIB … 5-35, 5-38
neighbor … 5-33
neighbor data remaining … 5-70
neighbor data, displaying … 5-65
neighbor statistics … 5-67
neighbor, maximum … 5-69
operating rules … 5-38
operation … 5-35
optional data, configuring … 5-48
outbound packet options … 5-36
packet boundaries … 5-35
packet dropped … 5-35
packet time-to-live … 5-37
packet-forwarding … 5-35, 5-69
packets not forwarded … 5-33
per-port counters … 5-68
port description … 5-48
port ID … 5-47
port speed … 5-49
port trunks … 5-39
port type … 5-47
refresh interval … 5-43
reinitialization delay … 5-45
remote management address … 5-38
remote manager address … 5-47
reset counters … 5-67
rxonly … 5-46
setmib, delay interval … 5-44
setmib, reinit delay … 5-45
show advertisement data … 5-63
show commands … 5-40, 5-42
show outbound advertisement … 5-63
SNMP notification … 5-36
SNMP traps … 5-36
spanning-tree blocking … 5-39
standards compatibility … 5-38
statistics … 5-67
statistics, displaying … 5-67
system capabilities … 5-48
system description … 5-48
system name … 5-48
terminology … 5-33
time-to-live … 5-36, 5-43
TLV … 5-34
transmission frequency … 5-36
transmission interval, change … 5-43
transmit and receive … 5-36
transmit/receive modes … 5-36
transmit/receive modes, per-port … 5-46
trap notice interval … 5-46
trap notification … 5-45
trap receiver, data change notice … 5-45
TTL … 5-36, 5-37
txonly … 5-46
VLAN, untagged … 5-70
walkmib … 5-38
with PoE … 3-12

**LLDP-MED**
displaying speed … 5-64
ELIN … 5-59
enable or disable … 5-36
endpoint support … 5-51
fast start control … 5-54
location data … 5-58
medTlvenable … 5-56
Neighbors MIB … 5-65
topology change notification … 5-52
Voice over IP … 5-50

**load balancing**
*See* port trunk.

**logging**
facility … C-27

**logging command** … C-33
syntax … C-27, C-36

**logical port** … 4-6

**loop, network** … 4-2

## M

**MAC address** … B-3, D-1
displaying detected devices … D-4
duplicate … C-11, C-16
learned … B-10
port … D-1, D-2
switch … D-1
VLAN … D-1, D-3
walkmib … D-3
**MAC authentication**
SNMP notification … 5-23
**Management Information Base**
*See* MIB.
**management VLAN**
*See* VLAN.
**management VLAN, DNS** … C-71
**manager access** … 5-10
**manager password**
SNMP notification … 5-14, 5-23
**MD5 authentication** … 5-6
**MDI/MDI-X**
configuration, display … 2-19
operation … 2-18
port mode, display … 2-19
**media type, port trunk** … 4-2
**MIB**
HP proprietary … 5-2
listing … 5-2
standard … 5-2
**mirroring**
*See* port monitoring.
**MLTS** … 5-34
**monitoring**
links between ports … 2-34
See port monitoring.
**monitoring traffic** … B-18
**monitoring, port** … B-18
**Multiline Telephone system** … 5-34
**multiple forwarding database** … B-6, B-12
**multiple VLAN** … 5-1

## N

**NANP** … 5-34
**navigation, event log** … C-23
**network management functions** … 5-3, 5-10
**network manager address** … 5-2, 5-3
**network monitoring**
traffic overload … B-18
**Network Monitoring Port screen** … B-17
**network slow** … C-4
**North American Numbering Plan** … 5-34
**notifications**
authentication messages … 5-14, 5-23
configuring trap receivers … 5-16
enabling for network security … 5-23
link-change traps … 5-14
network security … 5-23

## O

**operating system**
*See* switch software.
**operation not allowed, LACP** … C-6
**operator access** … 5-10
**OS**
version … A-18
*See also* switch software.

## P

**packet**
debug messages … C-28
**password**
SNMP notification … 5-23
SNMP notification for invalid login … 5-14
**pattern matching, show command output** … C-56
**PCM**
security concerns when deleting public community … 5-3
**PD** … 5-34
**ping** … C-69
*See also* DNS, resolver.
*See also* troubleshooting.
**ping test** … C-45
**PoE**
advertisements … 5-58
allocation, usage … 3-8
benefit of LLDP-MED … 5-50
changing priority level … 3-4
changing the threshold … 3-4
CLI commands … 3-10
configuring … 3-10

configuring operation … 3-4
configuring port priority … 3-7
data link layer … 3-13
disabling a port … 3-11
displaying LLDP port config … 3-14
DLC … 3-13
enable or disable operation … 3-5
fault … 3-10
IEEE 802.3at stnd … 3-13
LLDP detection, enabling or disabling … 3-12, 3-14
lldp negotiation … 3-13
manually configuring power levels … 3-9
negotiation … 3-13
operation on HP switches … 3-1
oversubscribed … 3-2
planning and implementation … 3-22
poe-lldp-detect command … 3-12
port-number priority … 3-4
power negotiation … 3-13
power supplies … 3-2
pre standard detect … 3-18
pre-std-detect … 3-5
priority class … 3-2, 3-4
setting allocation … 3-9
status … 5-54
supporting legacy devices … 3-5
TLVs … 3-13
using LLDP … 3-12
viewing power status … 3-18

**poll interval**
*See* TimeP.

**port**
address table … B-10
blocked by UDLD … 2-35
broadcast limit … 2-17
CLI access … 2-6
configuration … 2-1
configuring UDLD … 2-35
context level … 2-15
counters … B-7
counters, reset … B-7
duplex, view … 2-7
enabling UDLD … 2-36
MAC address … D-2, D-3
menu access … 2-2
monitoring … B-17
monitoring, static LACP trunk … B-18
speed, view … 2-7
traffic patterns … B-7
transceiver status … 2-13
trunk
*See* port trunk.
utilization … 2-12
CLI … 2-12
web browser access … 2-21

**port configuration** … 4-1

**port names, friendly**
configuring … 2-29
displaying … 2-30
summary … 2-28

**port security**
port trunk restriction … 4-2
trunk restriction … 4-6

**port trunk** … 4-1
bandwidth capacity … 4-1
caution … 4-2, 4-7, 4-14
CLI access … 4-9
default trunk type … 4-8
enabling dynamic LACP … 4-13
enabling UDLD … 2-36
IGMP … 4-6
limit … 4-1
limit, combined … 4-16
link requirements … 4-2
logical port … 4-6
media requirements … 4-5
media type … 4-2
menu access to static trunk … 4-7
monitor port restrictions … 4-6
monitoring … B-17
nonconsecutive ports … 4-1
port security restriction … 4-6
removing port from static trunk … 4-12
requirements … 4-5
SA/DA … 4-22
spanning tree protocol … 4-6
static trunk … 4-5
static trunk, overview … 4-3
static/dynamic limit … 4-16
STP … 4-6
STP operation … 4-5
traffic distribution … 4-5
Trk1 … 4-5
trunk (non-protocol) option … 4-4
trunk option described … 4-21

types … 4-4
UDLD configuration … 2-35
VLAN … 4-6
VLAN operation … 4-5
web browser access … 4-14
*See also* LACP.
**port trunk group**
interface access … 4-1
**port, active** … 5-33
**port-access authentication**
SNMP notification … 5-23
**port-based access control**
event log … C-6
LACP not allowed … 4-18
troubleshooting … C-6
**port-utilization and status displays** … 2-12
**power levels, configuring** … 3-9
**Power-Sourcing Equipment** … 3-3, 5-34
**pre-standard detect** … 3-18
**priority class**
defined … 3-2
**prompt, =>** … C-61
**PSAP** … 5-34
**PSE** … 5-34
**PSE, defined** … 3-3
**Public Safety Answering Point** … 5-34
**public SNMP community** … 5-3, 5-10

## R

**rate display for ports** … 2-12
**Reset button**
restoring factory default configuration … C-61
**reset port counters** … B-7
**resetting the switch**
factory default reset … C-60
**restricted write access** … 5-10
**RFCs**
RFC 1493 … 5-2
RFC 1515 … 5-2
RFC 2737 … 5-38
RFC 2863 … 5-38
RFC 2922 … 5-38
RFC 3176 … 5-28
*See also* MIB.
**RIP**
broadcast traffic … 2-17
debug messages … C-28
**RMON** … 5-2
**RMON groups supported** … 5-28
**routing**
traceroute … C-49

## S

**savepower**
command … F-1
port-low-pwr … F-1
show led … F-1
**SCP/SFTP**
enabling … A-8
session limit … A-12, A-14
troubleshooting … A-13
**secure copy**
*See* SCP/SFTP.
**secure FTP**
*See* SCP/SFTP.
**secure management VLAN, DNS** … C-71
**security**
enabling network security notifications … 5-23
**Self Test LED**
behavior during factory default reset … C-61
**serial number** … B-3
**setmib, delay interval** … 5-44
**setmib, reinit delay** … 5-45
**severity level**
event log … C-17
selecting Event Log messages for debugging … C-42
**sFlow** … 5-2
agent … 5-28
CLI-owned versus SNMP-owned configurations … 5-29
configuring via the CLI … 5-29
destination … 5-28
sampling-polling information … 5-31
show commands … 5-29
**SHA authentication** … 5-6
**show**
custom option … 2-8
displaying specific output … C-56
exclude option
show
begin option … C-56
include option … C-56
interfaces brief … 2-7

interfaces config … 2-7
pattern matching with … C-56
tech, custom … A-22
**show cpu** … B-4
**show debug** … C-31
**show interfaces**
dynamic display … 2-8
**show interfaces display** … C-56
**show management** … 1-8, 1-17
**show tech** … C-53
custom … A-22
**show-tech** … A-21
**slow network** … C-4
**SNMP** … 5-1
ARP protection events … 5-14
authentication notification … 5-14, 5-23
CLI commands … 5-10
communities … 5-2, 5-3, 5-10, 5-11
configuring with the CLI … 5-12
configuring with the menu … 5-11
mapping … 5-9
configure … 5-2, 5-3
configuring security groups … 5-20
configuring SNMPv3 notification … 5-20
configuring SNMPv3 users … 5-19
configuring trap receivers … 5-16
configusing trap receivers … 5-16
DHCP snooping events … 5-14
different versions … 5-14
enabling informs … 5-18
enabling network security traps … 5-23
enabling SNMPv3 … 5-19
fixed traps … 5-16
invalid password in login … 5-14
IP … 5-1
link-change traps … 5-14, 5-24
manager password change … 5-14
network security notification … 5-23
notification, LLDP
SNMP notification … 5-36
public community … 5-3, 5-10
supported notifications … 5-14
system thresholds … 5-16
traps … 2-35, 5-2, 5-14
walkmib … D-3
well-known traps … 5-16
**SNMP trap, LLDP** … 5-45
**SNMPv3**
"public" community access caution … 5-4
access … 5-3
assigning users to groups … 5-5
authentication, configuring … 5-6
communities … 5-9
enable command … 5-5
enabling … 5-4
encryption, configuring … 5-6
group access levels … 5-8, 5-9
groups … 5-7
network management problems with snmpv3 only … 5-4
restricted-access option … 5-4
set up … 5-3
users … 5-3
**SNTP**
broadcast mode … 1-1, 1-10
broadcast mode, requirement … 1-2
configuration … 1-3
disabling … 1-11
enabling and disabling … 1-9
event log messages … 1-23
menu interface operation … 1-23
operating modes … 1-1
poll interval
*See* TimeP.
selecting … 1-2
show management … 1-8
unicast mode … 1-2, 1-11
unicast time polling … 1-22
unicast, deleting addresses … 1-23
unicast, replacing servers … 1-23
viewing … 1-3, 1-7
**software**
*See* switch software.
**software image**
*See* switch software.
**software version** … B-3
**source-port filter** … 2-26
**spanning tree**
fast-uplink, troubleshooting … C-11
problems related to … C-11
show tech, copy output … C-54
using with port trunking … 4-6
**SSH**
enabling or disabling … A-10
TACACS exclusion … A-11
troubleshooting … A-13, C-11

**standard MIB** … 5-2
**statistics** … B-2
**status and counters menu** … B-2
**switch software**
download using TFTP … A-2
download, failure indication … A-5
download, switch-to-switch … A-17
download, troubleshooting … A-4
download, using TFTP … A-2
software image … A-1
version … A-4, A-15
**Syslog**
"debug" severity level as default … C-42, C-44
adding priority description … C-40, C-41
compared to event log … C-26
config friendly descriptions … C-39, C-41
configuring for debugging … C-29
configuring server address … C-27
configuring server IP address … C-33
configuring Syslog servers and debug destinations … C-27
control-desc … C-39, C-41
displaying Syslog configuration … C-31
event log messages sent by default … C-38
logging command … C-33, C-35
operating notes … C-43
overview … C-26
priority-descr … C-40, C-41
*See also* debug command.
sending event log messages … C-26
server configuration … C-37
severity, "debug" … C-35
specifying severity level events for debugging … C-42
specifying system module events for debugging … C-42
user facility as default … C-39, C-44
using event log for debugging … C-27, C-36
**system information** … B-3
fans … B-3
power-supply … B-3
temperature … B-3
**system module**
selecting event log messages for debugging … C-42

## T

**TACACS**
SSH exclusion … A-11
**task monitor** … B-4
**taskusage -d** … B-4
**taskUsageShow** … B-4
**Telnet**
troubleshooting access … C-3
**TFTP**
copy command output … A-24
copy crash data … A-25
copy crash log … A-26
copy event log output … A-25
copying a configuration file … A-21
copying software image … A-19
download software using CLI … A-5
downloading software using console … A-2
switch-to-switch transfer … A-17
troubleshooting download failures … A-4
using to download switch software … A-2
**threshold setting** … 5-3, 5-10
**thresholds, SNMP** … 5-16
**time format, events** … C-17
**time protocol**
selecting … 1-2
**TimeP**
assignment methods … 1-1
disabling … 1-20
enabling and disabling … 1-18
poll interval … 1-20
selecting … 1-2
server address listing … 1-8, 1-17
show management … 1-17
viewing and configuring, menu … 1-15
viewing, CLI … 1-17
**timesync, disabling** … 1-20
**time-to-live, LLDP** … 5-36
**TLV** … 5-34
**TLVs, mandatory** … 5-70
**traceroute** … C-69
asterisk … C-51
blocked route … C-52
fails … C-50
**traffic monitoring** … 5-3, 5-10
*See also* sFlow *and* RMON.
**traffic, monitoring** … B-18
**traffic, port** … B-7
**transceiver**

error messages … 2-14
view status … 2-13
**transceivers**
configuring when not inserted … 2-33
not inserted … 2-33
**trap**
CLI access … 5-16
configuring trap receivers … 5-16
security levels … 5-17
**trap notification** … 5-45
**trap receiver** … 5-2, 5-3
configuring … 5-16
sending event log messages … 5-17
sending SNMPv2 informs … 5-17
SNMP … 5-16
up to ten supported … 5-16
**traps**
authentication trap … 5-23
auth-server-fail … 5-23
enabling network security notifications … 5-23
fixed … 5-16
link-change … 5-23, 5-24
login-failure-mgr … 5-23
password-change-mgr … 5-23
port-security … 5-23
*See also* notification.
snmp-authentication … 5-23
threshold … 5-16
**troubleshooting**
approaches … C-1
browsing the configuration file … C-52
configuring debug destinations … C-27
console access problems … C-2
diagnosing unusual network activity … C-3
diagnostics tools … C-44
displaying switch operation … C-53
DNS
*See* DNS.
fast-uplink … C-10
ping and link tests … C-45
restoring factory default configuration … C-60
spanning tree … C-10
SSH … C-11
SSH, SFTP, and SCP Operations … A-13
switch software download … A-4
switch won't reboot, shows => prompt … C-61
unusual network activity … C-3
using CLI session … C-27
using debug and Syslog messaging
using the event log … C-17
viewing switch operation … C-52
web browser access problems … C-2
**trunk**
*See* port trunk.
**TTL**
LLDP … 5-36
**Type-Length-Value** … 5-34

## U

**UDLD**
changing the keepalive interval … 2-37
changing the keepalive retries … 2-37
configuration … 2-35
configuring for tagged ports … 2-37
enabling on a port … 2-36
event log messages … 2-39
operation … 2-35
overview … 2-34
supported switches … 2-35
viewing configuration … 2-38
viewing statistics … 2-39
warning messages … 2-39
**unauthorized access** … 5-23
**undersize packets** … 2-27
**Uni-directional Link Detection**
*See* UDLD.
**unrestricted write access** … 5-10
**unusual network activity** … C-3
**up time** … B-3
**URL**
HP … 5-2
**USB**
copy command output … A-24
copy crash data … A-25
copy crash log … A-26
copy event log output … A-25
**users, SNMPv3**
*See* SNMPv3.
**utilization, port** … 2-12

## V

**version, OS** … A-18
**version, switch software** … A-4, A-15
**view**

duplex … 2-7
port speed … 2-7
transceiver status … 2-13
**VLAN**
address … 5-1
configuring UDLD for tagged ports … 2-37
device not seen … C-15
event log entries … C-18
link blocked … C-11
MAC address … D-1, D-3
management and jumbo packets … 2-25
management VLAN, SNMP block … 5-1
monitoring … B-1, B-17
multiple … 5-1
port configuration … C-15
secure management VLAN, with DNS … C-71
switch software download … A-2
**VoIP**
LLDP-MED support … 5-50

## W

**walkmib** … 5-38, D-3
**warranty** … -ii
**Web authentication**
SNMP notification … 5-23
**web browser interface**
troubleshooting access problems … C-2
**web site, HP** … 5-2
**windshell, debug destination** … C-28
**write access** … 5-10

## X

**Xmodem**
copy command output … A-24
copy crash data … A-25
copy crash log … A-26
copy event log output … A-25
copying a configuration file … A-22
copying a software image … A-20
download to primary or secondary flash … A-16
using to download switch software … A-14

Technology for better business outcomes

To learn more, visit www.hp.com/networking

© Copyright 2012 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.

November 2012

Manual Part Number
5998-3456